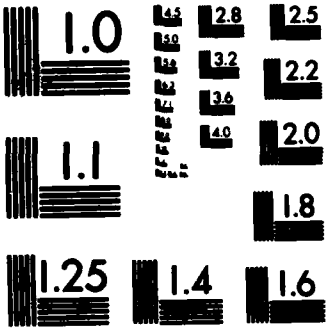
AD-A143 015 CLASSIFICATION MANAGEMENT JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY VOLUME 19 1983(U) NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ROCKVILLE MD 1/2

UNCLASSIFIED E SUTO ET AL. 1984 F/G 5/2 NL




MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD-A143 015

# CLASSIFICATION MANAGEMENT

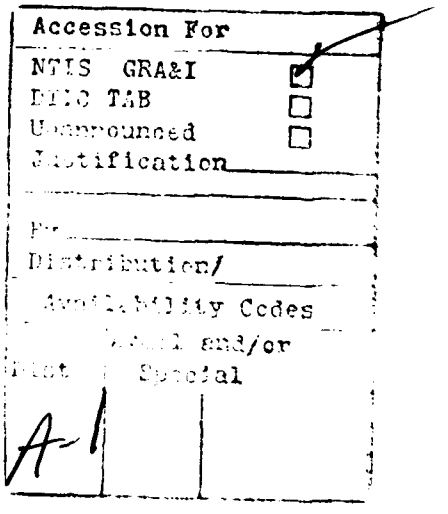




C

M

# CLASSIFICATION MANAGEMENT


JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XIX 1983

ISSN-0009-8434

Published by the National Classification Management Society. Mailing Address: Executive Secretary, NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editors of this volume: Eugene Suto and DeLoris Goldsby. 

# TABLE OF CONTENTS

## PART ONE — Proceedings of the Nineteenth Annual Seminar (INFORMATION SECURITY INSIGHTS)

## PART TWO

# PART ONE

# Proceedings
# of the
# Nineteenth Annual Seminar

## 21 - 23 June 1983

## Americana Hotel
## Fort Worth, Texas

*KEYNOTE*

**L. Britt Snider**
**Director**
**Counterintelligence and Security Policy**
**Office of the Under Secretary of Defense**
**Department of Defense**
**Washington, D.C.**

It's a pleasure for me to be here with you in Fort Worth at the NCMS 19th Annual Training Seminar. Certainly, gathered by the reports that you heard here this morning, NCMS is alive, well and kicking and is going to stay that way. I think Jerry Acuff, in particular, and Brad Bradfield are to be congratulated for putting together this program which is really an impressive one that covers a number of very timely and significant issues in the security area. I'll be mentioning a few of these this morning. Hopefully, I won't duplicate the remarks of some speakers that follow. I was talking to Steve Garfinkel before the seminar and he plans to cover part of what I'm going to have to say this morning, but in more detail. I understand he's already passing a pop quiz for the participants here. In any case, there may once have been a time when security seemed a rather mundane, mechanical enterprise. When we faced threat, we accepted it on good faith and we dutifully went about all the prescribed motions in order to protect against it. It was left to individual departments and agencies and their respective contractors to develop and enforce the rules. Certain areas were deemed so sacrosanct that change seemed out of question. Nowadays, particularly within the last two years, I see within the executive branch a much greater emphasis on centralized review and the development of uniform policies in the security area. Old policies and procedures are being called into question and new ideas, which I think once were thought impossible to achieve, are being debated and, in fact, are being implemented. Further, there has been, in my view, a much better development of the threat that we face from our adversaries. We understand better today that we need to protect against hostile agents. We also need to protect against technical collection capabilities from the air, the sea and from space. We also have a better appreciation of some recent work in the intelligence community to the extent that our adversaries are capitalizing on the openness of our Society to improve their own military capabilities. I want to use my short time with you this morning to mention several recent developments which I think demonstrate these points. I'll begin with National Security Decision Directive 84 (NSDD 84), which was signed by President Reagan on March 11, 1983. The expressed purpose of the Directive was to deal with leaks of classified information to the press. This Presidential Directive will have repercussions far beyond the area of leaks.

The new Directive imposes requirements in five areas. First, it requires non-disclosure or secrecy agreements for persons holding both collateral clearances and Sensitive Compartmented Information (SCI) accesses when in the Executive Branch. Second, it directs the Attorney General to undertake a review of federal policy in the personnel security area. Third, it provides that departments and agencies change their regulations as appropriate to permit adverse actions to be taken against employees who refuse to take a polygraph examination in the course of an investigation of an unauthorized disclosure of classified information. Fourth, it requires departments and agencies to adopt appropriate policies to govern contacts with the media. Fifth, it requires departments and agencies to institute programs to identify unauthorized disclosures, investigate them, and then deal with the culprit if and when he is found. I want to take a couple more minutes with the first three of these. As I mentioned, the Directive requires non-disclosure agreements of employees with both collateral clearances and SCI accesses. Although it is still somewhat premature for me to discuss the details of these agreements, a proposed SCI agreement contains a requirement that employees with SCI access submit materials for prepublication review that may contain SCI. It is not our intent in DOD, however, to impose a prepublication review requirement as part of the collateral agreement. Moreover, we plan in DOD to implement this requirement of the Presidential Directive on a prospective basis with the new non-disclosure agreement taking the place of the briefing statement that contractor employees are now being asked to sign. We do not contemplate that any persons who already have a security clearance or SCI access sign the new forms, but rather we will gradually bring this requirement into the DOD system. With respect to the review of Federal

Personnel Security Policy, the Attorney General has convened a high level interagency working group under the chairmanship of Mary Lawton who is council for Intelligence Policy of the Justice Department. Their task is to review and revise Executive Order 10450 and also Executive Order 10865 which, as you know, governs the industrial security area. There have been a number of attempts over the years to rewrite and revise these very old documents, but they've all failed. However, this time I believe their effort is going to succeed primarily because the President has told them to do it. It has gotten the attention of the top level policymakers in the government. In talking to Mary, she predicts this is going to take some time and she hopes by the end of this calendar year to have the final product. Of course, this is likely to cause reverberations down the line in all of our personnel security policies and programs.

I mentioned the polygraph aspect of NSDD '84 and although it's relatively a minor part of the whole document, it has certainly attracted the most attention. It has also had its impact on the Defense Department's plans to change its own polygraph policies. Although the NSDD only addresses use of the polygraph in the context of a leak investigation, it reverses long established rules in most agencies that adverse administrative action will not be taken against employees solely on the basis of their refusal to submit to a polygraph. This feature has caused the most commotion in the press and Congress and in fact we invigorated the concerns in both quarters in what DOD was intending to do. For those of you who are unfamiliar with the DOD proposal, let me quickly summarize. The key feature permitted DOD components to establish a requirement for a limited conterintelligence scope polygraph examination as a condition of access to special program information. I emphasize it would not require such examinations, but would only permit them, if in the judgment of the component agency concerned the sensitivity of the information justified such extraordinary precautions.

It's very interesting to take note of the British Commission established to review the espionage case of Geoffry Prime who had been assigned to GCHQ, the equivalent in the British government of NSA. You are all probably aware of the case already. Among other actions, the Commission recommended to the British government that a pilot program be instituted utilizing polygraph examinations as a condition of access to extremely sensitive government information. Subsequently, Prime Minister Thatcher approved this recommendation, defending in a very candid way to the Parliament the need for the program. Let me read the statement she made to the Parliament. It's interesting. "The polygraph is the only measure of which it could be said with any confidence that it would have protected GCHQ from Prime's treachery, either because it would have deterred him from applying to join or would have exposed him in the course of examination. In view of this and the extreme gravity of damage caused by Prime, the government accepts the Commission's recommendation that a full and thorough pilot scheme should be carried out. The Commission recognizes that a polygraph examination would be seen by some as an unwarranted invasion of their privacy, but we are dealing with matters of the highest national security and those who have access to the nation's most sensitive secrets must expect to be subject to the most rigorous screening procedures. Moreover, the commission proposes that questioning under the polygraph should be limited to counterintelligence examination, such as, exposure to approaches by hostile intelligence services, and questions of lifestyle such as criminality, drug taking, sexual matters and financial affairs. They also recommend that in no case should a supposedly adverse polygraph indication treated by itself as grounds to withhold clearance without independent confirmation from some other source. The government is in full agreement with the Commission that safeguards of this nature must be incorporated into the pilot scheme." That's the end of the quote. I read that to you because I think it's pretty remarkable that the British government has done this. In fact, I would be interested in hearing from some of our colleagues here from Great Britain on the subject. I wonder how many polygraph machines there are in the UK. I don't think there are many, but in any case, it's noteworthy because it parallells precisely what the Defense Department was proposing to do last fall. It's sort of coincidental that it has come along at this time. This report, incidentally, was made available to Secretary Weinburger for his perusal.

Speaking of the DOD proposal it was recently returned to components within DOD for a second round of coordination. If they continue to support the proposal as they did last summer it will probably be submitted to the Secretary in a few months.

So much for the polygraph and status of NSDD '84. I think Steve Garfinkel plans to cover NSDD '84 in some detail after lunch.

I now want to turn your attention to the new NSC framework. It has been about a year now that it's been in existence. In any case, the new NSC level framework has been established to deal with counterintelligence and security matters. Since all of you may not be aware of this development, I'll tell you a little about it.

Last August, the DCI, Mr. Casey, acting as Chairman of the Senior Interagency Group for Intelligence, which is a cabinet level body, created two sub-committees-The Interagency Group on Counterintelligence, which is chaired by Judge Webster, the FBI Director; and the Interagency Group on Counter Measures (IGCM) which is chaired by my boss, Deputy Undersecretary for Policy, Richard Stillwell.

The Interagency Group for Counterintelligence focuses primarily on matters relating to counterintelligence operations, investigations and awareness. Each of the military departments, as well as the CIA and the FBI, sit on this Committee. It would not be appropriate for me to go into great detail on what this committee has done. They have met eight or nine times and produced a number of reports. Even for this short period of existence they've demonstrated that they are a very useful forum for the discussion and resolution of matters in the counterintelligence area.

I can say a bit more about its companion group, the Interagency on Counter Measures. Defense chairs this committee, with the members coming from the CIA, State, Justice, FBI, Commerce, Treasury, NSA, and DIA, as well as the three military departments. The jurisdiction of this interagency body extends to virtually every security program and activity of the government, from information security (the subject of particular concern to you) to technical programs, such as TEMPEST, as well as the mechanisms we have to warn of the existence of technical collection platforms being opposed against the U.S. W[illegible] the Committee has relied upon existing Interagency bodies to review particular programs and activities to the extent possible, I think it has served to motivate policy review and stimulate thinking that probably would not otherwise have been done. The IGCM started out last September with 17 separate initiatives. Several of these are still in progress. Several have concluded with no changes recommended, and several have actually gone to Judge Clark with a recommendation that they be addressed in some form of national policy issuance. Until such issuances are forthcoming, I feel it would be inappropriate for me to discuss their substance. The groups have reviewed U.S. policy in such areas as the overflight of U.S. territory by communist bloc civil aircraft, operations security, tempest requirements in the United States, restrictions on COMSEC monitoring, restrictions on U.S. firms owned by foreign interests who are in classified business with the government, and other topics of that nature. The IGCM is completing a report of virtually all government and security programs and activities. We have approximately 20 different programs that are being described from an organizational standpoint. The report is intended to serve as a base line from which future adjustments in the organizational structure of these programs can be evaluated and conducted. It also represents the first time that we've pulled together all of this information in one place. At this point it's classified. I am hoping that we can produce an unclassified report. It can have widespread use in the security community.

With the creation of the Interagency Group on Counter Measures there is for the first time an interagency body at the NSC level which has broad jurisdiction over security matters for the entire government. To date, it has been active and productive and in the near future I would expect you would begin to perceive the results of some of its efforts. The same point can be made with respect to both bodies which taken together form something of a milestone, particularly in the area that we are all involved in. Indeed, it's difficult for me to see why it took so long for such forms to be established. I would be a strong advocate of retaining this sort of structure in the future, regardless of what political party might be in power.

A third area I wanted to touch on is some of the activities currently under way in defense to counter the loss of significant military technology. I understand you will be hearing from Mead Field from Customs about Operation Exodus, which has been an unqualified success. I know some of the other speakers are talking about other aspects of the problem. I wanted to confine my remarks to ongoing efforts with the idea to deal with the problem of controlling the availability of such technology within the U.S. DOD has been grappling with this thorny problem for several years now, and at last, I think we're beginning to make progress. As you recall, our first approach to the problem had been to resort to the classification system to protect the information in question.

Recognizing limitations imposed upon the use of such information which is classified, we attempted to have our cake and eat it too by proposing a fourth level of classification. This level would have imposed very minimal safeguarding controls for the protection of information, which would have been primarily military technology classified at the fourth level. We would call that restricted as you may remember. Ultimately, this effort failed within the Executive Branch. We are now considering a somewhat different approach.

In December of last year, we contracted with a firm called Advanced Technology Systems for a study of the control of unclassified military technology. Its principal author is the esteemed Arthur Van Cook. He has done a good job in setting forth the problem and in creating solutions to it. This is how he summed up the problem in this report — "There has been and continues to be a significant loss of valuable U.S. unclassified technology with military applications. It is easily acquired by our adversaries, thus providing them the means to increase their military potential to the detriment of U.S. national security interests. In our open Society it is neither feasible nor desirable to control totally this body of important information. Consequently, we must set our priorities and protect that which we possess in ways that are both practical and appropriate. A coherent U.S. program to control the loss of unclassified technology with military applications must be established.

First, the laws that impact on the control of this valuable data must be amended to make them compatible rather than working against purposes. Next, government must identify that information which is determined to require protection against public disclosure and foreign access with a far greater degree of precision. Within DOD and its contractors mechanisms need to be established to insure that uniform and comprehensive controls are imposed over the information in question. In this connection, it should be noted that whatever system of controls is implemented, it is likely to be ineffectual without full cooperation of both government and industry."

While this approach has yet to receive approval within defense, I think Art VanCook's book does indicate that there is general agreement in industry that defense controls on the disclosure of technology should be imposed apart from the classification system. There seems to be general agreement that technology to be protected under any such scheme ought to be that whose military significance is demonstrable and which we know are needed by our adversaries but they cannot be obtain elsewhere.

As I mentioned, DOD is at present reviewing this proposal. If it's adopted it would apply to components and our contractors and at this time it is drafted in a way that it would generally prevent the dissemination of designated military technology outside the government and its contractors without the permission of the Defense Department.

Integral to this approach would be the ability to withhold this type of data from requestors under the Freedom of Information Act. Only if classified can we withhold it now, despite the fact that an export license would be required to export it outside of the United States. Indeed, once such data has been approved for public release by a government agency no export license is required to send this technology out of the U.S. Someone called that a "Catch 22." We are attempting to deal with this problem by suggesting new legislation. Defense proposed in the last Congress an amendment that would exempt the technical data that would be subject to export controls from disclosure under the Freedom of Information Act. The administration supported this amendment

and it was eventually part of the bill that passed the Senate last summer. However, no action was taken on the House side. This same exemption in modified form is now in the Senate bill 774 which was introduced by Senator Hatch. We are hoping that it will come to a vote on the Senate floor sometime in late July. Then we can attack the real problem-the House side. We are hopeful that this effort will take care of this problem that we perceive and feel it closing a gap in the regulatory framework for this sort of data.

These are some of the reasons that my in-basket is overflowing these days. My perception is that we are busier and probably more productive than we've been in a long time. Certainly, there seems to be a greater interest in our work at higher levels in the government and in Congress than we've had before.

Our task, it seems to me, is simply not to provide more security, but to improve our security and provide better security. I think it's a simple matter just to suggest measures that would give additional security assurance. I think it's far more difficult to evaluate security requirements in terms of a demonstrative threat of the resources that are available to cope with it in the operational needs of the government agency or defense contractor for whom we work. This seems to me is what we're there for. I think we advocate our responsibilities as security professionals if we do not make this sort of analysis and cast our recommendations accordingly. Yet, I run against this one-dimensional thinking all the time. In any case, I would encourage each of you to take a broader view which I think will make you a far more valuable employee to your particular organization.

In closing, let me say how much I appreciate having the chance to come here and get together with all of you. I'm sorry I can't stay. It shall be my loss. These sort of conferences give us a chance not only to view old acquaintances, but also to give us a chance to reflect a bit on what we do on a day to day basis. That is a luxury these days. I wish you all a very successful conference, and I would be pleased to see any of you when you are in Washington. Please stop by the office. Thank you.

## *DEFENSE INVESTIGATIVE SERVICE OVERVIEW*

**Thomas O'Brien**
**Director**
**Defense Investigative Service**
**Washington, D.C.**

Good morning Ladies and Gentlemen. It's indeed a pleasure for the Defense Investigative Service (DIS) to have the opportunity again this year to participate in the seminar of this Society. I say that because, in our view, this Society is totally professional and totally devoted to the kinds of things the Defense Investigative Service is responsible for. We feel that the work you do in education and bringing to the attention of people the happenings in classification management is vital to the successful administration of the Defense Industrial Security Program. We will have a panel here a little later this morning with representatives from DIS. I think at that time we'll be happy to entertain your questions.

This afternoon, Jerry Crane, the Deputy Chief at DISCO will give you a briefing on DISCO and then tomorrow morning, as previously announced, we will have workshops-one concerning the DD form 254 and the other one on Classification Markings. These workshops have proven to be very successful as part of the management seminars that the Defense Industrial Security Institute conducts both in Richmond and around the country. We felt that it would be worthwhile to bring to the attention of this audience the opportunity to participate in these workshops. So we're very, very pleased to have that opportunity.

We have four of our classification management specialists with us-Sheila Daigle from the San Francisco region; Jim Lydon from the Philadelphia region; Mary Jo Hickey from Los Angeles; and Frank Hucker from Boston. Later, I'll explain why we don't have the other four here.

### *DIS OVERVIEW*

I'm very happy to report that DIS is very much alive and well. DIS has grown to a fairly sizable organization these days. We have an annual budget of over 100 million dollars! We have a staff now of over 3400 people located in some 300

locations around the country. Of course, we also have an office in Brussels, Belgium.

When I was reflecting on what I should cover this morning, I was trying to think and pinpoint what is probably the most important thing, or the best thing that's happened at DIS during the past year or so. Without a great deal of thought it occurred to me that our best achievement is the spirit of cooperation that has resulted from the amalgamation between our industrial security responsibility and our industrial security people, on the one hand, and our personnel security investigation staff on the other (our special agents and our investigative operation). We now have amalgamated these two functions into a very coordinated unit all working as a team. Many of our offices are co-located around the country. Our agents and our IS reps are talking together. So when the agents go into a facility, he is able then to relate back to the IS rep things that he sees and hears. The IS rep does the same thing. We're working as a team and together we're able to accomplish a great deal more than was ever possible when industrial security was administered separate or apart from the investigative function. We feel that this is clearly our greatest achievement.

Those of you who were at the seminar last year may remember that we showed some charts and the charts related primarily to the investigative backlog that had developed over the past several years in DIS. This year I have no charts because we have no backlog, I'm very pleased to report. You may recall that we had charts that showed DIS about 18 months ago had pending some 84,000 cases. Today, we have just 34,000 working cases. So we've completed about 50,000 cases. We've got them out of our system. Every day in DIS we open up about 800 cases. The volume is staggering. We are now at a point where we have no backlog; we're on a current basis. The most important thing, of course, is not how many cases we have pending, but how long it takes us to get them completed. Some 18 months ago it was taking us over 180 days, on the average, to complete the case. For the past month, for those cases where we had DIS jurisdiction only, where we do not have any overseas leads, we have been averaging 66 days. Our goal is 65 days. We are not quite there, but we feel quite comfortable in completing those cases on an average of 66 days. For those cases where we have overseas leads the military department supports DIS overseas, because we do not have investigative resources abroad. Those cases were completed on average in 71 days. We feel that from the investigative standpoint we're very healthy. This is important.

Last year the Department of Defense convened a special panel called the "Blue Ribbon Panel" to review the entire spectrum of personnel security policy. They came up with several significant recommendations. Their recommendations were based on a very significant finding-a finding that's not a surprise, but they focused attention on it. That is the fact that when you look at espionage cases over the recent past and indeed over the distant past in almost every instance the individual who was involved in espionage was not so involved at the time he was investigated, adjudicated and cleared. His involvement with a foreign intelligence apparatus developed after he was initially investigated and after he was initially cleared, and he was placed in a place or position of trust or responsibility where he had access to our classified information. One of the primary recommendations of the "Blue Ribbon Panel" was that we should develop a system for periodic reinvestigation of those people who have access to our most sensitive information. We now have such a program in effect.

On the first of April we began periodic reinvestigations. Some of you who were involved in sensitive department intelligence information know that in the past and under the Director of Central Intelligence Directive 1/14 there has been a system for periodic reinvestigation of people with SCI access. But that was a rather perfunctory, on-the-record investigation. Now, beginning on April 1, all people who have access to SCI and all people who have a top secret clearance will be subject to a periodic reinvestigation about every five years.

We have never had, prior to this time, a reinvestigation program for people with top secret clearances. Obviously we couldn't begin immediately to reinvestigate all of those people. Indeed, the Department of Defense does not really even know how many people we have cleared top secret. In industry we do. DISCO has precise rec-

ords and we know exactly how many people we have in our cleared facilities with our top secret clearance. The military departments do not have this type of tight, centralized system. Therefore, we don't really know precisely what the workload is. We do know how many people have SCI access. But we're going to start, and we will be conducting about 40,000 periodic reinvestigations each year. Now these investigations will be far more detailed than the past reinvestigations of people with SCI access.

Our investigations periodically will consist of a national agency check, local agency checks and all the areas where the person has lived, worked and gone to school for at least the past five years. We will do a national credit check. We will do an employment investigation. We'll verify employment; talk to co-workers; talk to contemporaries, peers of the individual; and, most importantly we will conduct an indepth interview of each subject.

The indepth interview, I'm sure that all of you are aware of this, which was developed some 18 months ago, is part of our new concept in background investigation-the so-called interview-oriented background investigation. That was a major step forward in improving and enhancing our investigative product. We've been doing that now for over 18 months and the results have been absolutely astounding. Even those who were most enthusiastic about the interview-oriented background investigation are amazed at how successful we've been. We're happy now to bring that in as a part of each of these periodic reinvestigations.

The way this is working, especially so far as industry is concerned, DISCO will send out requests to the facilities asking that those persons who have been selected now for the periodic reinvestigation to complete a new set of personnel security questionnaire and fingerprint cards. Essentially, it's the same as the new clearance application. When DISCO receives those new forms, we then will conduct this reinvestigation. For people with SCI access, the contracting activity will advise the contractor of those people who are to submit the forms. Those forms will be submitted to DISCO and then we will process the people for the reinvestigation. This is a very significant step forward and improvement in our whole personnel security process. It's also a good management help for the Defense Investigative Service. In the past, DIS has been subject to tremendous peaks and valleys in terms of new requests for investigation. We, of course, have no control over requests for investigations. On the periodic reinvestigation systems we set up a quota system so that when initial requests for clearances and investigations are up we will dole out lower quotas. At those times of the year when initial requests are up we'll give fewer quotas. This way we can keep our level of work at a fairly constant level. This is not only good from a security policy standpoint, but it is also good from a DIS management standpoint.

Another major improvement, and also a result of this "Blue Ribbon Panel," is beginning the 1st of July this year. In another week or so, we're going to replace the interview-oriented background investigation (IBI) with what we now call the enhanced IBI. In each case we are going to give significant additional coverage. The new IBI will be, in our opinion, the best personnel security investigation now available throughout the federal government. We're looking toward the end of this year to develop a single scope background investigation so those people that have SCI access as well as people with top secret clearance will be subject to the same type of a background investigation. We're looking ahead and making great strides in improving personnel security overall.

In DIS we've done a lot of other innovative things. Today, we have our special agents aboard naval aircraft carriers. I only mention that as an example of the kinds of things we're doing to get our investigation completed in a very timely way, as I was saying, in currently 66 days on the average.

One of the most significant things we've seen over the past several years is the tremendous increase in the number of personnel security clearance requests. As you know, DISCO processes all of our industrial security clearances. In fiscal year 1981, DISCO issued 161,000 clearances. In fiscal year 1982, DISCO issued 181,000 clearances. This year to date, if we continue at our same pace, we will issue somewhere between 203,000 and 204,000 clearances, which repre-

sents a 27% increase in fiscal year 1983 over fiscal year 1981. The numbers are just staggering. We, of course, relate that to the fact that more and more of our weapons systems are involving higher and more critical technologies. All of this translates into higher classifications and more needs for higher clearances and more clearances.

When we talk about clearances we also have to talk about clearance denials. We have developed some backlog at DISCO and in the Industrial Personnel Security Clearance Review Directory which is part of the Office of the General Council and the Office of the Secretary of Defense. There are a number of cases pending in both of those areas.

One of the problems we've had is that most of those cases, some 34%, involve use of marijuana. The policy, with respect to when do we issue a clearance and when don't we issue a clearance when marijuana is the issue, has been kind of a gray area. The Department of Defense has resolved this question. Essentially, the new policy that's recently enunciated goes something like this: "Where there has been infrequent use of marijuana in the past, and the body of evidence developed from the investigation supports the conclusion that the individual will not continue to use marijuana in the future, then we will issue a security clearance, as a general rule. On the other hand, where there has been infrequent use of marijuana in the past, but the evidence based on the investigation suggests, or supports the conclusion that the individual will continue to use marijuana in the future, then as a general rule, we will not issue a security clearance and we will withdraw security clearances of people of this type that have been issued in the past." Before, that's been gray. Note I use the word infrequent use in the past. If there's been more consistent use in the past, then there has got to be stronger evidence that this use is indeed stopped. But basically, people currently using marijuana will not be cleared by the Department of Defense. We want to publicize that. We want people to know that. We want people in your facilities to be well aware of the fact that if they are bound and determined to break the law on the use of marijuana, they're not going to be cleared by DOD.

Now let me turn to the other part of our responsibility, the administration of our cleared facilities throughout the country. Here again our numbers are up. Today, we have over 12,000 cleared facilities. That's more cleared facilities than we've had any time since the mid-1960's. Just two years ago we were just slightly over 10,000 cleared facilities. In the past two years we've been increased by some 2,000. Again, we attribute this to the more sophisticated weapon systems, the higher technology and the higher classifications. Despite this, we have now reached the point where we are conducting our scheduled inspections on time for 98% of the time. Last year, when I addressed this group we were slipping inspections. We were only making some 75-80% of our scheduled inspections on time. But in the past year we have reversed that, we've turned it around, and we're now 98% plus on schedule.

Equally or even more important, we're finding that during the course of our inspections we are, indeed, getting more quality into the inspection. We're doing this in a number of ways. Number one, we're spending more time in the facility. We monitored this very closely. We know how much time in each category of facility we spend on average in the inspection, and when our times are up. We're going in more and more with teams. It's not just an IS rep in a large facility, but it's a team of IS reps backed up and supported by classification management specialists, by education and training specialists, by ADP specialists and the other body of support that we have in our Security Offices. We're finding a definite improvement.

We're also well underway on a program that was started over a year ago of unannounced inspections. At the present time, we're conducting over 10% of our Industrial Security inspections on an unannounced basis. When this idea was originally broached there was great concern that this would be disruptive and would be harmful. Further, it might even tend to breach this partner relationship that exists, and exists so well, between our industrial security people and you in industry, our counterparts. But it hasn't done that. We found that those facilties that are conducting consciencious industrial security programs in their facilities have no concern about unannounced inspections. As a matter of fact, I've had a number of security supervisors tell me

that they're kind of glad to see that. It just makes them feel good to let that IS rep arrive at the door unannounced and find, indeed, that things are working well. On the other hand, we do find that those few, and believe me it's few, contractors who intend to cut the corners and take the easy way out. We identify those problems and are able to then correct the problem, make believers or in some rare cases, where the problem is not really correctable, get the people or the facility out of the system. We're finding again this has improved the overrall quality of our industrial security apparatus.

There are certain areas where we are directing special attention. I want to quickly review those for you.

One is the long standing requirement that the contractor report whatever questionable or adverse information comes to your attention concerning one of your cleared employees. This is a very important requirement and a very important concept. Too often, when we think of a security clearance, we think about that initial request, that initial investigation and then the clearance is issued. That is only the beginning. The real important thing about a security clearance is yes, we take a person that we've ascertained to be reliable, loyal and trustworthy, but then we put him into an atmosphere, a climate, into a system where his security performance can be monitored. When a problem develops, something comes to the attention of management that suggests maybe we need to look again. Maybe there's a financial problem. Maybe there's an alcohol problem. Maybe there's a marijuana problem, or any one of a number of problems. We need to look at this kind of a situation and therefore, for many, many years there has been this requirement in paragraph 6B of the Industrial Security Manual that you the contractor report to DISCO when questionable or adverse information comes to your attention. What we're looking for in the course of our inspections is to insure that each facility has a system to make these reports. Our COG offices and IS reps now are working more closely with DISCO so that each time the IS rep goes into your facility, he knows what reports you've made during the last year or, if you've made none. Those facilities that haven't made a report in paragraph 6B of a year or more, that at least makes us more attentive to this area. If we have a facility with some 5,000 people, and over the past year there hasn't been a particular problem with any of them, we're gonna be looking pretty hard to see "Are you the contractor complying with the reporting system." Now, it's particularly important when a contractor terminates employment. If you fire somebody because of a problem, it's very important that you report this to DISCO because he has a transferrable clearance. And if you fire somebody you say, "Oh, I've solved that problem." I don't have to report it. But if that individual goes and gets a job at another cleared facility, he tells that facility he's got a clearance (and he does). That cleared facility asks for a transfer of clearance. DISCO is unaware of the problem, and it just automatically transfers. We rely heavily on you to pass that information to us so that we can prevent transfer of clearances where we have a problem. IS Reps are going to look at your system. Is there something set up with your medical department, personnel department, and other departments of your facilities to make sure that the security director is getting that information so he can make the required report? This is a most important requirement.

Another area that we're stressing very hard is that requirement that governs unclassified information relating to classified contracts. Of course, we view the Industrial Security Program as kind of the keystone of the government's effort in this fight against technology transfers, or illegal technology transfers. Obviously, the most sensitive information that must be protected is the classified information that's subject to the controls of the Industrial Security Programs.

In paragraph 5o, as you're all aware of, is the requirement that before you publish any information, be it classified or unclassified, relating to a classified contract you must have a DOD approval as prescribed. Your DOD form 254 tells you to whom you go and in the last analysis it comes under the Public Affairs Office of the Office of Secretary of Defense.

Too often in the past, people have tended to not regard that requirement as too significant, and contractors have tended in promotional and sales literature and at symposiums and conferences, to present information without having it

checked. We checked, of course, to insure that there's no classified information embodied in that. Then we also check it to insure that there's not information subject to export controls that would be released. Once something gets into the public domain, that obviates the provisions of the Export Control Act in the International Traffic and Arms Regulation. Paragraph 5o is very high on the agenda of each IS rep during each 696 inspection.

A third area of special attention involves those 5,500 cleared industrial personnel that are permanently assigned abroad. As I mentioned earlier, when we cleared somebody, we put him in a cleared environment, a facility. But the kind of exception to that rule, is the 5500 cleared industrial personnel permanently assigned overseas. They are not attached or working at a cleared facility. They're in a more hostile environment, where the opportunity for espionage and loss of classified information are greater. And, generally speaking, our monitorship or control is less. We're stressing this much more. Again our IS reps are cooperating with DISCO. When the IS rep goes into your facility, he or she knows how many cleared personnel that are pursuant to your facility clearance are permanently assigned overseas. We're going to ask you why they need a clearance overseas. We're going to ask you where they are. Often we find that an individual has moved several times and the DISCO record does not reflect his current whereabouts. We're going to double-check that.

Most importantly, we're going to ask you when was he briefed and by whom. We're discouraging these "by-the-mail" briefings. We think that if you just send a person a piece of paper and say, "Here's all the security things. Sign it." It's a very profunctory act. He really doesn't get to the heart of his security responsibilities. He really doesn't get motivated in terms of what he's supposed to do security wise. We're strongly encouraging that you brief these people face-to-face. Bring them back. Or, at least insure that they attend the many periodic briefings that our Industrial Security Europe office conducts at all convenient points throughout Europe and the Middle East. So stress this to your people. Make them go to these briefings. It's not only to their benefit, but to yours as well.

As I said earlier, in our Industrial Security Program, we look at the IS rep as the heart of our system of administration. But he is not alone. He is backed up by a very good and meaningful support system. As I said, we have classification management specialists. We have ADP specialists in each of our regions. We have education and training specialists and a whole staff of staff specialists that back IS reps. So when he goes in, if he doesn't have a problem or the solution to your problem right there, he's got the people backing him that will provide that kind of a solution.

Just let me touch very briefly on a couple of other matters. Many of you are involved in our Industrial Facilities Protection Program or Key Facility Program. Others of you are involved in our program for the safeguarding of sensitive arms, ammunitions, and explosives. To make our system more effective, we're centralizing those responsibilities. So, henceforth, all IS reps will not be looking at IFPB and Arms Ammunitions Explosives. We're going to have specialists in each region to concentrate in that area, and get special training. They will be handling those special programs. We think we can do that more effectively and more efficiently.

I'm frequently asked "When are we going to see the new COMSEC supplement to the ISM?" The old one is so old that I don't remember how old it is. We've been talking at several meetings for several years. I'm very pleased to report that we now have reached a general accord between our offices in DIS, between NSA, and between the Office of the Secretary of the Defense. We've worked out all the details, and all the areas of disagreement. OSD is now just putting the final touches on that supplement. They will be sending it to DIS within the week or so, and we will have it printed some 90 days thereafter. By late summer, early fall at the latest, you should have the new issue of the COMSEC supplement.

Finally, let me just mention OPSEC. I know there's going to be some panels here later on on that. But the Department of Defense for the first time is about to issue a DOD directive governing OPSEC across the board. Insofar as OPSEC and industry is concerned, that directive will contain three very significant policies.

Number 1: OPSEC can only apply to classified information in contractor facilities. The problem of unclassified information will no longer be governed by OPSEC requirements in industrial facilities.

Number 2: All OPSEC requirements will be specifically provided for in the contract document. What you have to do will be spelled out in your procurement contract. Otherwise, you don't have to do it.

Number 3: All inspections and follow up by DOD will be handled within the framework of the Defense Industrial Security Program by the Defense Investigative Service.

We think that those three steps will solve the "OPSEC problem". We're pleased with that policy development.

In closing, just let me make a pitch. I mentioned earlier the names of the four classification management specialists from our regions that are here. The reason I didn't mention the other four is because they're vacant positions. I'm going to do a little sales pitch-a little recruiting pitch now. We have four very good positions available. One in our Washington region; one in our Atlanta region; one in St. Louis; and one in Cleveland. These are GS-12 positions and we have time to have the announcements open. We can hire, through one announcement, current government employees with status. We can also hire, through another announcement, people who work in industry and have CM experience who do not have government status. So, if you are interested in a very lucrative, a very challenging, a very rewarding position, in a great organization, let me strongly encourage that you talk to us. Dick Williams and Sandy Waller have copies of the announcements and all the details. I'm very serious about this. We feel that this is the best place in the world that we can recruit for these very key positions. As I mentioned earlier, we consider these to be very key positions in our overall team concept to Industrial Security Administration. And, very frankly, we've been very hard pressed to get the kinds of people we want. In the past, a lot of times, we've taken good, talented IS reps and made them CM specialists. But that is not the best way to go. It's much better to take a person with good classification management experience, and then bring them in to the DIS operation and organization. So, again, let me stress and encourage any of you who might be interested in great employment in Washington, D.C., Marietta, Ga., St. Louis, Mo., or Cleveland, Ohio, please see either myself, Dick Williams or Sandy Waller and we will be more than pleased to give you all the details.

Again, thank you very, very much and I wish you a great seminar.

*DEFENSE INVESTIGATIVE SERVICE*
*CURRENT AREAS OF INTEREST*
*(DIS PANEL PRESENTATION)*

**Dick Williams**
**Chief, Industrial Security Programs**
**Defense Investigative Service**

The Defense Industrial Security Program is one of the most active security programs in government and it's the one that many of you look to in providing primary guidance in the area of Industrial Security. It is a team program-one that we have worked together for many years. What makes this program good is the fact that we do work together. I think that the primary thing that has improved the program over the years is the input we've received from professional organizations such as NCMS. The function of the Defense Investigative Service is to administer the DISP in industry and in the user agencies. Regarding the user agencies, we have added one which is the General Accounting Office.

I'd like to talk a little bit about our organization and the way it's put together. First of all, we have our Director, Tom O'Brien, who you've already heard from. He has two principle program managers. This is a new concept that Tom has installed. I think that he brought it with him from the Navy. That is the Program Manager concept. He has a Program Manager for Industrial Security and that's Dan Dinan, and then we have a Program Manager for Investigations. He administers the program from a regional level to our regional directors. Lloyd Kelly, of course, is the Regional Director here with us today for Industrial Security. We also have the Defense Industrial Security Institute (DISI).

Many of you have been to this fine institution. I hope that you have enjoyed the classes.

At headquarters Dan Dinan has this type of structure. We have a headquarters staff under the chief of this program division that's responsible for developing and implementing policy. Then we have the Industrial Facilities Protection Program Division and the Program Standard Division which is our operational group that actually relates to the region on operational matters. Then we have our two primary field extensions. DISCO, you'll hear from later on, and our Office of Industrial Security International. We have some information that we are going to provide on that at a panel on Thursday.

In the regional Director office that we have around the country we have two directors. The Director of Investigations and the Director of Industrial Security. Lloyd will talk a little more about that. He has a Facilities and an Operations Division Chief. For those who are contractor personnel you have already related to many of the people in these positions. I'm only going through this by way of review because I was told that this is a training seminar.

The publications that we primarily have responsibility for are the Industrial Security Manual for safeguarding classified information (DOD 5220.22M), which many of you are quite familiar with. On the user agency side we have the Industrial Security Regulation (ISR). Of course, with the Industrial Security Manual we have the various supplements.

We go through seven steps of coordination which we've altered a little bit and recently streamlined. This is primarily the work of Tom O'Brien and Maynard Anderson. They've gone a long way towards helping streamline the way that we coordinate changes and improve the overall timeliness of the coordination process.

First of all, we check with OSD to let them know the types of things that we're going to coordinate. Then we go out after we develop the change to the user agencies. I would like to tell you at this time that we now include your Society in this coordination process. The Council for Defense and Aerospace Industries Association (CODSIA) is the designated contact coordination point for industry. However, we accept input from NCMS and the other organization that was mentioned. We have received some excellent comments on some of the change packages. I'd like to compliment you on the professionalism that you have in your Society as evidenced by the outstanding comments that we've received in some of our change packages. It has been very, very helpful to us.

I'd like to talk now about future trends and some of the things going on in the Industrial Security Program.

The first one that Tom has already mentioned is the COMSEC supplement. There's a quote from the Bible that says, "Faith is the evidence of things hoped for." We've been hoping for a COMSEC supplement since we started this coordination process in February of 1980. We have reworked that thing quite a number of times. I believe it now embodies the consensus of the views of government and industry. Obviously, we're going to have certain disagreements as we coordinate any package and it's our sincere hope to have the COMSEC supplement on the street in the very near future. We have quite a few change packages in coordination at this time. We have approximately 32 Industrial Security Regulation changes, and we have approximately 37 Industrial Security Manual changes. One of the things that we have done that is a tremendous improvement in the coordination process, is to shortstop it. Coordination process is something I've been greatly concerned with since I was an IS rep down in Orlando, Florida. I used to say, "What is wrong. Why does it take so long to get those packages out. It takes them a year." Now I can't figure out how they did it in a year. Of course, Tom was in my position then. Maybe that improved the process. But basically it's a very time-consuming process. The solution that we've come up with is when a policy is already embodied as National Policy, whether it happens to be COMSEC policy, or whether it's DOD Directive, or Instruction, or in some other format such as the International Publications, NATO CM5515 Final, or the UCN 69 or UCN 70, it really doesn't serve a whole lot of purpose to go through massive coordination channels. In other words, you already have the essense of the materials you're supposed to

incorporate into our publication. I think the best evidence of how we can make this work is the new Executive Order 12356. We used the information that we had from the Information Security Oversight Office (ISOO), and we called in a select industry group and worked with them. We worked with some of the user agency personnel, and we went and implemented it as quickly as we could without going through our standard, lengthy coordination process. It's our intent that whenever we have the opportunity, try to accelerate this process. I think that's absolutely critical in making the Industrial Security Program a viable program. When our policies lag and the policy that's put out officially is two to three years old it loses the overall thrust we want it to have. Our purpose is to make those policies that we put into place more current with the current thrust that's happening in the Industrial Security environment.

Talking about future trends, Tom has already struck one and that is the growth of the program. The program has greatly picked up. We still have, as near as we know, about 12 million documents in industry. The majority of the classified material that's developed for the government comes from industry. We still have the majority of the classified material in about 5% of our large facilities. These facilities, which many of you are from, have professional security staffs (people who are involved in administering the program for many years-very professional people). Some of you are from the medium-sized firms which are not in that 5%; some of you may even be from the small ones where our education efforts have to be more extensive than they would have to be in some of the larger firms. Tom mentioned the change we've had of the interview-oriented background investigation. I would request that you work with us when we do these investigations by providing a space for the interview to be conducted. Help us out so that we can work together. I could say that that's required by the Industrial Security Manual, but I won't say that. I'll just solicit your help and ask you to help us. This would be very useful to us in expediting the obtaining of the investigative information we need to further decrease the time that it takes to conduct investigations.

We have a current problem that's very important to the nation. That's technology transfer. It's something that Britt Snider has already mentioned. This is something that we've got to work together on. You can help us here by insuring that when your personnel go to seminars to give presentations, if there's information that (1) relates to a classified contract, that it is cleared with tne user agency before it's released. Don't wait until a week before a seminar to send that in to the user agency and expect an immediate response, because as you've read in the paper sometimes that response means you don't send your people to seminars. So work with us on this. We've got to stem the tide and flow of technology out of the United States. When our adversaries can take information in the form of products from this country and then return them for repair under a warranty, I think things have gotten a little in excess. We definitely need your help to work with us and to insist that the information which is released is released properly. Of course, Dr. Smalldone will talk on Thursday about the export requirements.

Some of the other things that I'd like to talk about is the future trends that are contained in the new Industrial Security Letter. I'm going to very quickly run through these. We have new DOD 48 and DOD 49 Security clearance forms. I hope you will use these forms. We project these can save you thirty minutes on filling out the forms and I certainly hope that you'll request them from DISCO. When you've filled the forms out, please don't mail them to DIS headquarters. I'm getting in hundreds of forms that should be going to your cognizant security office. The COG security office is the authority for your geographical territory. Please work with our COG Offices.

Another thing that I would like to talk about very briefly is that we have a problem of Communist countries buying U.S. firms. Each cognizant security office has a list of these firms. It's classified and we'll share this information with you if you believe you're being involved with some of those firms.

I would like to also mention the reemphasis on Classification Management. We've developed what we call a revised procurement partners presentation that will be given to user agencies shortly. It's our intent to revitalize the CM function. Everybody laughed when Tom gave his pitch

to have some of you join us. You know if you want things done right, sometimes you should do it yourself. Here's an opportunity for at least four of you to help. We need good people in government and we would love to have some of you join us. We think it would be quite lucrative for you but perhaps not up to what you might be making in the industry, but think of the job satisfaction you'd get out of it. Without you laughing we would love to have you with us and we hope some of you will join us, because we're looking for professional people. You know, you can take an IS rep and I've been an IS rep, many of the others here who represent DIS have been IS reps, and you could say, "Now you're a CM specialist." If you haven't been in a user agency I can tell you that sometimes making a classification guide and just looking at one in the field are two different things. So we need your help and we would love to have some applications from some of you that are well qualified. We certainly are looking forward to receiving those. This is the professional organization that is involved in the classification function. Therefore, we're coming to you and we really would appreciate help in this area. Thank you very much.

**Lloyd Kelley**
**Director**
**Industrial Security**
**San Antonio Region, Defense Investigative Service**

When I was asked to speak very briefly on the items of interest at the region level, my intention was to bring to your attention those things that we're putting stress on during our facility inspection program. Mr. O'Brien and Mr. Williams, respectfully, between them covered those. I'll chat with you about another item of even more paramount importance to myself and my seven colleagues around the country.

It's been with us for seven or eight years now and will be with us for a few yet to come. That's our personnel resources. During the past roughly eight years, in the COG office side we suffered about a 75-80% attrition rate in our work force throughout the ranks, and not from the loss of defecting disenchanted people but actually the reverse. The COG office system, when it came into being and grew to its present size between the early 50's and very early 60's, was populated by World War II vintage people of generally the same age bracket. About 1974 or 1975 they started retiring. Boy, they went in droves. We have a situation right now where probably 80% of our work force of IS reps in the plants have 3-5 years experience in the business. In all honesty, ladies and gentlemen, when dealing with plants like those represented here they're still on a learning curve. You know you're participating in the training. Our highest priority in the region right now is to continue to recruit, to train, and to develop the IS rep work force. We hope to replace the losses with good people, and to develop them with that combination of program knowledge, objectivity, and a very difficult to achieve balance between enforcement and assistance that Mr. O'Brien has talked about repeatedly. We are there to survail and enforce the DOD security requirements but also, in all sincerety to assist you in accomplishing those requirements.

Having had the bulk of what I was going to say snatched away, I'm going to depart from my subject if the boss doesn't fire me, and speak of a subject dear to the hearts of the goals and purposes of this Society. A classification concept that came into being and has grown, sometime while I wasn't looking, increasingly in the past year or two. I have seen repeatedly the application to the classifications concept as relates to hardware. Wherein the hardware is classified at a lower level than the information that can be disclosed through custody and analysis of that piece of hardware. When I was a bright young man learning the in's and out's of this job, more than a few years ago, I was taught that hardware was classified at the level of information that could be obtained from it. As a very simplistic example of what I am talking about, I saw a classification guide on a missile guidance unit a few days ago. The fuse-occilating frequency was secret and the occilator confidential. Even a ham radio operator like me can check that little rascal at a test bench and tell you in five minutes what the frequency is. I don't understand that concept and I would invite, through the course of this seminar, our user agency colleagues to enlighten me on it. I would encourage all of you when you come across this kind of a problem to resolve it directly with the user agency, and if you are unsuccessful, to bring it to my classification management specialist. Surface those problems either to the inspection

team or to the CM specialist when he or she is out with the team, or by letter, telephone, etc. to the region headquarters. I think there's a problem out there we need to look more closely at and surface with good factual data to the policy levels for resolution.

**Sandra Waller**
**Industrial Security Specialist**
**Defense Investigative Service**

We're still having the same problems with the DD254. We're also still having problems with marking. I have just come to the conclusion that no matter how hard we try and how hard we work, we're going to always have the same problems and we might as well just learn to roll with the punches.

We have workshops tomorrow on marking and the DD 254 and I hope you will try to attend one or the other of those. If you have had all you can stand of the workshops in the past on the DD254 and the marking guide, sleep in tomorrow morning and then come down bright-eyed and bushy-tailed for the next session. We've got a lot of criticism on having some of the same thing over and over and over again in the Society and in our training sessions. But you have to remember that this is a training session and a lot of people are here because they don't know how to prepare a DD254 or they don't know anything about markings and they came here to learn.

Last year when we were at this seminar I showed you what the Industrial Security Manual looked like in a draft. We don't have a new ISM again this year at the printer's. I think we are planning to issue another ISM sometime after the first of each year instead of changes throughout the year.

One of the things that I think you folks will be interested in that we are working on at DIS headquarters is that we are trying to revise the information that is in the Industrial Security Manual on the preparation of the 254 to include some illustrations and more detailed guidance on what we mean by some of the questions we ask, especially in item 11 on the 254. We're also planning for the user agencies to include the instructions for the preparation of the 254 in the Industrial Security Regulation.

Everyone by now has gotten the last ISM and has seen the rewrite on paragraph 11, the marking requirement. We've not really gotten a lot of questions about this new rewrite on paragraph 11 and I'm not sure if that's a good sign or not. It could mean that you have just given up in questions because it just cannot be written so you can understand it. If you still have problems with the marking requirements, Shiela Daigle will have her workshop tomorrow on marking requirements. I'm sure she'll be able to answer every question you have.

I would like say one thing about the changing marking requirements. We have been criticized, sometimes rather harshly, on the changes, the constant changes, that we have made to the Industrial Security Manual marking requirements. First, we say you mark it this way, and then that way, and we have flip-flopped back and forth. I agree we have flip-flopped back and forth, but it was because of the changes in the Executive Orders that we have flip-flopped in an effort to try to stay consistent with what the Executive Order requirements are. If there is another change in the Executive Order, we will change them again. We're just going to have to do it, and try to stay consistent. The pamphlet that was put out under the Executive Order 12065 that was modified for Industries use will not be reissued under Executive Order 12356. We have decided to try to put an appendix into the Industrial Security Manual with illustrations and samples of the marking requirements for contractors instead of issuing the little marking pamphlets. We're hoping to do this so that you will be able to extract the appendix and make a little hand out to give in your Security agency plans. We will not be issuing the pamphlet itself.

**Questions and Answers**

Q: I'm Liz Heinbuch with the Dept. of the Army. I'd like to ask Tom a question about something he said. First of all, several times you mentioned marijuana. What's the policy as far as other drugs are concerned. Was that significant that you referred only to marijuana?

A: Of course, the policy has been clearer with respect to the other drugs. If there has been use of so-called 'hard drugs' then the issuance of a

clearance is far more unlikely. Certainly, we have not been clearing people who continue or plan to use 'hard drugs' in the future. The only time we would clear a person that has a history of 'hard drug' use is when there's been a significant period of refraining from the use of the drugs and it's quite clear that the person has been clearly rehabilitated.

Q: Then the same policy would apply?

A: Yes.

Q: One more question. When you talked about the SCI and the top secret clearance requirements, that is having the same investigation for *both,* does that apply also to the government?

A: Yes. That same policy of reinvestigation applies equally to people in the military, civilian employees of DOD and contractor personnel.

Q: Will the scope of the investigation for an SI and OPSEC clearance be the same now?

A: Yes. The plan is by the end of the year to have a single scope. There are still details to be worked out on that. We tentatively hope by January to have those details worked out and have a single scope that would apply to everybody.

Q: We get so many people, especially military, that have a top secret SCI clearance and have not had the special background investigation. We wait a lot more than 66 days to get it done.

A: Let me just clarify that. In the case of the Army, we send the investigative results to the Army Central Clearance Operation. For Industry Personnel the investigative results are sent to DISCO. From the time you would submit the request to DISCO, it has to be processed to our personnel investigation center. Then the investgation is closed and then sent back, so the investigative time for top secret is about 66 days.

Q: You mentioned the new COMSEC supplement coming out. We've been having a running battle with one of our project managers on this matter. We do not have any CRYPTO equipment. I was told by our IS rep that we do not need a COMSEC account in order to get COMSEC documents. We are being told by the user agency contracting officer, 'Yes, you must have a COMSEC account.' Now I've got all the people in the group briefed on COMSEC. Is this going to be clarified? It's definitely *not* clarified in the present COMSEC supplement.

A: It does clarify. Essentially, if it has telecommunications security (TSEC) nomenclature, then it's in a COMSEC material control system. Therefore, you must, in those instances, have an account. You've got to have a custodian and all the things that go with it. There are some types of COMSEC information that are not captured in the COMSEC material control system. And those types would not be accountable in the COMSEC that you have been told about. Now we have some NSA representatives here that may like to add to that. But essentially, that came from the National Policy and that has now been embodied into the revised COMSEC supplement. One of the problems we had with the COMSEC supplement, that has drug this thing so long is that there's a National publication called NCSC-9. That gives the definitions. Unfortunately, a definition is depending on where you set on what it means. What we're trying to do now is to insure that both the government and industry are on the same wave length regarding these definintions. And one of the things we have done is to clarify those definitions to remove this doubt as to what should and should not be captured. This ties into a lot more than just capturing into the accountability system. It captures into additional safeguarding requirements you may have if it's in an account or if it's not in an account. There's a lot of other things regarding BI requirements on the custodian and the security officer. So the point that you have brought up is well taken and is addressed in the new supplement.

Q: Now you're saying that it is possible if you're only going to need access to certain documents, you may need a COMSEC account—even if you never get a CRYPTO document?

A: It depends on what is embodied in that document. If that document has TSEC nomenclature the answer would be yes. If it does not, it would depend.

Q: We received, out of the clear blue sky, five COMSEC documents from DTIC. So, he was quite

surprised. Because he was insisting that for all COMSEC documents he needed to open a COMSEC document account.

A: That has been a misunderstanding that has been in industry since...I used to inspect accounts. One of the things that we've tried to do is to clear this up by taking the National definitions that are contained in NCSC9 and it's our hope that by putting that in and the coordination that we've had with NSA that we've worked out this difficulty. That will be solved by the COMSEC supplement. If it's not, after you read the new COMSEC supplement, please write me a letter through your COG office and we'll certainly try to get it cleared up.

Q: Joe Reynolds, Sanders Associates. Recently, we came across a visit request from a naval installation for an individual who was born in Vietnam and is a U.S. citizen. The thing that brought it to our attention is that his security clearance was an emergency secret clearance, issued in April of this year. Have we come up with a new clearance?

A: No. We have not. Was it issued by DISCO?

Q: It doesn't say, Tom. It just says, "An Emergency Secret, April, 1983."

A: Well, on something like that, if it's a contractor employee, you ought to check back with us, because something is amiss.

Q: It's a government employee.

A: You ought to check with the government activity because something is still amiss. Whenever you see something that looks dumb, don't just say, Gosh!

Q: I hate to say it but we've already been back to the Navy and it's still an emergency secret. So we'll have to go to a higher level.

A: There's something wrong. Mistakes are made in a big program, and whenever you see something that doesn't look right, question it. We have to work together. If you see something that seems to be amiss, let's try to get to the bottom of it. Because something is wrong there. I don't know what it is, but something is wrong.

Q: We understand that also.

Q: I'm Mike Lower from Hughes Aircraft Co., El Segundo, Calif. and I want to direct this question to Dick Williams. Concerning the COMSEC supplement, over the past number of years, we've all gone back to our respective companies or agencies with the assurance that the new supplement is the mill, it's in print, it's in the mail, whatever. Can you, at this time, describe some of the major changes that are going to be forthcoming in this new supplement. We have a number of COMSEC accounts and a like number of custodians and alternates. Each time we go back that's one of their principle questions, "What's new that's coming down the pike?"

A: O.K. If you like, I'll give it a shot to try to capture some of the essential elements. I just gave that speech at Las Vegas and I really didn't bring that particular briefing. Essentially, some of the definitions are changed. This may seem like a minor step but those that were present at the Orlando meeting know that this is not a minor step. This is a major thing that has come up regarding the COMSEC supplement. We've got to insure that industry and government are on the same wave length in that when we state something we're using the same basic frame of reference. I think we've pretty well captured that. There is a change in that paragraph 37d is changed to delete the reference to paragraph 37e provisions. Specifically, this changes some of the relationships that we have in there. We have, I think, a clearer delineation on what should and should not be in a COMSEC account. We have clarification on transmission, exactly when a contractor can and cannot transmit COMSEC documents, how they're transmitted. We had great and lengthy detail discussions over whether or not a two-person rule ought to be used to transmit documents; whether or not a contractor must own their own aircraft in order to transmit a document; or whether or not they could lease an aircraft and still control that aircraft and transmit documents. There was lengthy discussions over who should control the COMSEC custodian. Originally the first concept that we are operating under which industry made comments on was that the

security officer had to have direct line supervision over the COMSEC custodian. That has been amended to where the COMSEC custodian has certain reporting requirments to the security officer, but does not directly report in terms of line authority. It's more or less a limited line, if you're familiar with those different terms, to the security officer. The security officer has overall responsibility. We had some clarification on the safeguarding requirements such as having to have secret safeguarding requirements applied to TSEC nomenclature information that is confidential and top secret safeguarding requirements to TSEC nomenclature that's in secret designated information. We have a clarification regarding the briefing form that we used to use. This is one of those areas you remember in my earlier presentation where things have moved on dynamically? What happened there was we received instructions from DOD to delete the certificate that we used for briefing. I've forgotten the number. I think it's 560-3. That has been deleted out. Originally, in terms of an ISL, that has been subsequently formulated and put into the COMSEC supplement. There's some thoughts now about coming up with some new briefing requirement. We suggest the contractors document the briefing on the back of the 482 form. That's just a real quick overview without going into specific details on the COMSEC supplement. One thing I'll promise you that we'll do and that is when we're close to coming out with the actual printing-when I see that it's about 30 days away-we'll put together an ISL that essentially enumerates the prime items of the COMSEC supplement. We'll try to get that on the street before or on the same time frame as the COMSEC supplement comes out. I know a lot of you are not involved in COMSEC because there's only about 273 of our contractors out of the 12,000 that are cleared. However, for the benefit of those of you who are involved, that's just a real quick overview of what's embodied in the COMSEC supplement.

Q: I'm Jack O'Neil, Security Manager, Draper Laboratories, Cambridge, Mass. The recent security bulletin referred to a classified list of Communist-owned countries and I think that Dick Williams alluded to it earlier. It seems to me that this might be more appropriately placed in the hands of a contractor. Are there any plans to do that as opposed to having it in the DIS office?

A: Let me read that ISL item. This will be the new ISL that's dated June. I hope some of you already have the copy that has been published. It says, 'Each of our eight COG security offices was recently provided a list of firms which were Communist-owned and are charted in the United States. The lists shall be used in our continuing security awareness effort as well as to provide contractors, information related to export control laws. In essence, what that says is that our cognizant Security Offices will make that information available to those contractors that are actively involved with relationships to firms that may be Communist-owned. The purpose that we have on putting this out (it is a classified document) is to make it available to our contractors. This is a change that's happened in the intelligence community over the years. Before intelligence people kept all that information and didn't share it with the operators. One of the purposes of this particular document is to share that with the contractors who actually need that information. So yes, we will share it with you.

Q: Pam Hart, ALM, Inc., Arlington, Va. This question is directed to Tom. I'm wondering if anyone else has this problem. The subject is adverse information. It bothers me to report this kind of information to you. I understand why you need it. We have many personnel advisors in our company that constantly are sending management people like myself to hire and fire seminars. It seems like every other month I'm in the Commonwealth of Virginia grievance meeting where I am the recipient of much wrath about termination, etc. Our policy in the company, if someone wants to verify a reference, is that we just say that they were employed during that period of time. We've had a lot of problems in this regard. Therefore, we have been instructed to not say anything derogatory at all. Whenever we approach management to report adverse information to DISCO they panic and they say 'just keep your mouth shut and we won't tell them anything.' When you start really applying pressure, particularly if, as you said earlier, we haven't had any report on adverse information for two years or whatever, how are you going to try to emphasize this to us. Are you going to do this in the exit

interview or could you possibly put out some kind of an official thing? I know it's in the Industrial Security Manual and I know that we've signed a security agreement, however, to emphasize this to top level management is that really our obligation?

A: Well, yes it is in the Industrial Security Manual, which is a contract. So that is the bottom line. We, perhaps, have been somewhat remiss in the past in that we haven't vigorously supported that particular requirement. There have been a series of articles on it in the Industrial Security Letter and 83L1 does cover it. Some contractors are concerned, because of the Freedom of Information Act and Privacy Act syndrome. That legislation probably did a lot more by inverse than it did by actuality. Certainly, I can see that as a general company policy, when some other employer comes to you and wants to verify a person's employment, you only do that and don't tell them that they were fired. That's something different. But you have a contractual responsibility with the Department of Defense to report adverse information for reasons I outlined earlier. Now the way we're going to get to reluctant management is to cite them for a major deficiency. And we're starting to do that. This is one of the things I eluded to earlier. We're working closely with our special agents and our IS reps and, very frankly, when a special agent is doing an investigation-let's say of an employee of yours that may have had a secret clearance at sometime and is now put in for a top secret clearance. If during the course of that investigation we ascertain that this person has had a problem, and the company has been involved in the problem, and it's never been reported, we will alert the IS rep to that problem. Then, he knows when a company has a problem. We're just going to cite it then as a major deficiency. And if a company says 'We're not going to report', we'll say "That's fine. It's your business." We'll just call them unsatisfactory and they'll no longer do classified work for the government. So we're very serious about this. We have to be. We don't to be mean, or I've heard it referred to as the *fink rule* and various asundry of things, but it's quite important that we get this information. As I said earlier, firing the person doesn't solve it because he can get a clearance somewhere else. So just think if you had adverse information on one of your employees and that person really turns sour and becomes involved in espionage and you haven't reported it. Talk to your management on those terms and how they want to cope with that problem.

Tom, could I add a word to this? Yes, Lloyd. Speaking from the COG office level, one of the roles of the IS rep should be plain in outbriefing management. This is one of the underlying reasons for the very long-standing practice of briefing top management. The IS rep, whenever this attitude that you describe exists, should be conveying to your management that it's the corporation who is signatory to the security agreement. It's management's responsibility. This is not your responsibility. It's not the responsiblity of the security officer or personnel officer to try to do this. It's management's responsibility. As Mr. O'Brien said when anything doesn't get done and it's significant, management of the corporation is held responsible. It's one of the things that we keep stressing to our people. This coming fall, during our meeting, I will stress this very important role in conveying this attitude to your management.

Having just gone through an inspection, Pam, where this was really stressed I would only add that what is clearly consistent with the National interests is really a judgmental call. I was asked from an industry point of view that maybe we can better define this big area.

We do have a proposed change that we have put together which we will be coordinating. It essentially outlines some of the elements that we consider adverse information from the DOD criteria. There's been a lot of insistance for many years from many of the user agencies and even in DOD itself to not put out something like that. The reason is that if we put out a criteria then the natural thing for people are to say those are the only things we have to report. Really, I think the point is the government must make that decision. The government made the decision to issue the clearance or not issue the clearance. The government must evaluate that information which comes into them that's adverse. We are going to try to get something together that will further clarify that."

Q: I'm Jim Hataway from NASA. My question concerns paragraph 11, marking requirements for

work in progress. As presently written, there's no requirement to portion mark any work in progress. I'd like to understand the reasoning why.

A: Well, we have had all sorts of agreements and disagreements and discussions on what is really required for marking papers. What we tried to do in paragraph 11, with the change in there, is to allow you the freedom to put together a working paper, or what is called a working paper or draft, without requiring the portion markings until you put it in your accountability system or you retain it for a certain length of time. This is because there are a lot of different ways that people put documents together. Some people will prepare the entire document and then they'll have a classifier or someone review the material and assign the paragraph markings. Other people, as they put it together, will portion mark each paragraph or portion. It was just to allow a little flexibility on how you mark on working papers. Do you have problems that you want to mark all working papers or portions as you go along?

Q: You enter work in progress if it's at the secret level 30 days after it's completion or when you reproduce it. Sometimes a project may work for a year and a half before you have a completed document. Would you consider that a vulnerability?

A: If you retain it longer than 30 days then you have to put it into your accountability system.

Q: That's wrong. It says 30 days after completion.

A: Thirty days after completion of the working paper.

That's true. It does say 30 days after completion. It also says that if you reproduce it you've got to put it into the accountability system. I think when you're looking at any type of project that's in development, especially if it's a new technology, source documents can be used to portion mark. Sometimes there aren't any source documents in new technology. For us to impose a requirement on all contractors that you must classify a document when in fact you don't know what the classification level is that technology embodies while you're processing and developing the document, would really not be realistic. That's the reason we have requirements stated that way. DOD has upheld that for sometime.

Let me just add a thought to that. You will recall that when portion marking originally went in there was a great deal of controversy. This happened to be one of the compromises. This is one of the areas where industry said it would be totally impractical to portion mark working papers; and this is part of the compromise. So maybe what we're hearing is 'Well, now that portion marking is an accepted routine procedure, we've got to go ahead and include it as part of the working paper requirement as well'. Is that what I'm hearing people say?

I see an awful lot of heads shaking no. We had a government representative at a very high level at OSD that was a large proponent of portion marking but now he's a contractor and he may have some different thoughts on it. I'll just mention that.

*ISOO Presentation*

**Steven Garfinkel**
**Director**
**Information Security Oversight Office**

First of all, I'd like to congratulate the seminar chairpersons, the new officers, and the old officers. I think we were all very impressed by that opening sequence. That was beautifully put together. Congratulations to you.

At any of these seminars there are always new people and so before I get into talking about Executive Order 12356 or the National Security Directive, I'd like to spend a minute or so talking about what ISOO is. The Information Security Oversight Office (ISOO) is an odd, little agency administratively located in the General Services Administration but taking all of its policy direction from the National Security Council. Our job is to oversee the Information Security Program throughout government. With a very small staff we do this in several ways. But most of all we do it by overseeing folks like yourself in government and industry. In other words, you folks are supposed

to do the work and we're supposed to come in and give you hell about it.

Among the activities that ISOO performs is a series of inspections, mostly located in the Washington, D.C. area because of limitation of travel funds. It would be great if we could travel more because everytime we do get somebody out there, we benefit greatly from it. We also collect and analyze data. The infamous standard form 311 that some of you are exposed to once a year. We receive and respond to all kinds of public complaints, appeals, objections; complaints that come from persons within government, outside government, congress, or where-have-you. We also participate in certain training activities. We hold many seminars and once in a while a symposium and we've even gotten into the business with 12356 of producing some audio-visuals.

One of the things I did want to mention while I was here is that at the mini-seminar in Washington, I mentioned the availability of our slide, tape and audio-visual presentations of 12356 which I think are quite good. We've gotten a lot of positive feedback from them. At the time, I recommended that everybody go ahead and order them from the National Audio-Visual Center. Unfortunately, we have had a lot of problems in getting out good reproductions of that slide, tape, and audio-visual program. The National Audio-Visual Center contracts out the work and we've had to get rid of several contractors for sending out inferior products. I'm very hopeful that that problem is alleviated now and if any of you are interested in it you'll inquire that the product you'll receive will be well worth the price. At the same time we are also using the Offices of the Defense Audio-Visual Agency to reproduce these things for defense agencies. For any of you who work for a defense agency, I know there are many of you, these things will be available through the Defense Audio-Visual Agency in the next couple of weeks.

Executive Order 12356 is, believe it or not, almost a year old. I think, looking back on it, I can summarize certain pluses over the course of this period of time and a few minuses as well. It's hard to believe that it's a year old and that the transition in almost every respect has been very, very smooth-the transition from Executive Order 12065 to 12356. If you read the new paper you thought there was going to be a clap of thunder on August 1, 1982, and the world would probably collapse. But, of course, none of that happened. Many people, perhaps too many people, don't even realize there's been a change.

Another plus has been what I would term the lack of instances of abuse. Much of the press criticism that 12356 received was tied to what was perceived by certain persons as the area's just ripe for abuse, areas involving overclassification of information that didn't deserve to be classified in the first place and reclassification of information that had been declassified and disclosed. If you'll recall, 12356 was intended to remedy certain perceived deficiencies in its predecessor. Unlike the string of Executives Orders that have preceeded it, it clearly was not another step in the direction of more open government. I think we could be honest about that and say, 'It was not another step forward'. Of course, the press and others perceived it as a giant step backwards and predicted all kinds of horrible things. I'm very pleased to tell you today that these horrible things have not happened. The agencies and industry have acted very responsibly in implementing this. I think for the most part just about everybody realized that we have improved the Information Security System through this new order, and it's there for us to screw up if we want to do the .

Another positive impact. There were several reasons behind Executive Order 12356. None of those reasons dealt with classifying more information. But there were some purposes to be served, obviously. Some of those purposes we're seeing are being served through the issuance of 12356. I'll just go through these very briefly. First of all, there were problems in litigating 12065 cases under the Freedom of Information Act. Especially, cases involving the balancing test where the agencies were being put to an ordeal that was never contemplated in the drafting and issuance of 12065. Well, we have been very successful in the courts with doing away with the balancing test just as we did away with it in the Executive Order. There was some fear that some courts looking at cases that had been filed before the change in the Executive Order would continue to insist on applying the balancing procedure and that has not happened. There was a very critical decision in favor of the government

in the D.C. circuit which, of course, is the most liberal in terms of openness in government in the U.S. Also, we have some indication, not a lot so far, that there is somewhat renewed confidence among our allies in our resolve in our ability to protect shared information. One of the major problems with 12065 was the problem of tone. Not that we couldn't protect the information, but that the Executive Order sounded so much like an extension of the Freedom of Information Act that we were unable to protect the information. I think those tonal problems have been largely resolved in 12356 and I think that is reflected in public perception, not only in the U.S. but elsewhere. Also, a number of the administrative problems with 12065 were areas where only the agency head could do something or only the agency head and the deputy head could do something. Those were just things that weren't running smoothly and have largely been corrected.

At the same time, there's the minuses that I hope will resolve themselves over time. For example, I'm very concerned that in many places we've been able to observe the reaction to the new Executive Order. Within government and within industry the reaction was very negative-not because of what the Executive Order said but just because there was a new Executive Order. This is very natural. I guess we can't expect that someone who's been working since 1970 in the security field, with their fourth new Executive Order, could look at it with rose colored glasses entirely. Obviously, these Executive Orders are part of the political process. It gets a little bit nerve-racking to think that this might be the case every time we have a change in administration. Nevertheless, I don't think that the real practical problems with implementing 12356 are so great that people have to shrink from its implementation. One of the other minuses we've been able to observe is that, especially in the military and because of its size, the word is not sufficiently out there about 12356. But there are activities that still have received no training whatsoever - - no *briefing whatsoever* on Executive Order 12356. This needs to be done and it needs to be done quickly. It happens that we're probably doing a better job on 12356 than we've ever done before in getting the word out as quickly as we can. But it's still not good enough. We see lots of areas where still the only information people have about Executive Order 12356 is what they've read in the papers. Largely, that's misinformation.

There have been a couple of areas where I would refer to them as minor abuses or just minor problems that fall within the area of taking advantage of the Order a little bit too much. For one, there's been too much use of the OADR duration marking. The Order provides that information is to be marked for declassification at a specific date or event if that date or event can reasonably be arrived at. Now we didn't do away with artificial automatic declassification on the assumption that those dates are easily arrived at in just about all cases. We knew better than that. We know that there are a limited number of situations when you are aware of the duration of sensitivity of information. But those instances do exist and the one thing that we're very concerned about is the *wrong* application of OADR for all classifications as if there's no way to classify information for a specific date of event, when that date of event is quite obvious.

Another thing that concerns us a little bit has been what I would consider the too many waivers of the portion marking requirement granted by agency heads. Executive Order 12356 allows agency heads to waive the portion marking requirement when certain tests are met or certain guidelines exist. The agencies that have waived the portion marking requirment, at least in their initial documents that have come to ISOO, have not abused 12356. Unfortunately, the word has gotten out in some of these agencies that the portion marking requirement has been waived and just about everything is being sent out without portion marking. That is not the purpose. The waivers were intended to be issued only when documents were closely held, and they were not being reproduced or sent out to other agencies. They were not the subject of large scale derivative classification. When documents are the subject of a lot of derivitive classification, or even a moderate amount of derivitive classification, it's deadly to deal with the document that's not portion marked. So we're trying to get with the agencies who have issued these waivers to see they are properly enforced.

The only other thing that I would consider a minus is the fact that in the middle of the transition to 12356, there was, issued by the President,

the National Security Decision Directive '84. I'm not going to criticize the Directive, that's not my purpose, however, the timing has hindered the implementation of 12356. It's largely hindered it because there's been much press play and so much attention drawn to the Directive. Much of our time has been spent in trying to implement the Directive that our time was taken away from the smooth implementation of 12356.

I'd like to spend a few minutes going over this little item that I passed out. Rick, unfortunately, gave you a bunch of the answers. Now, if we had coordinated it a little better, he could have at least given you the wrong answers. I might add in one or two cases he did. I'll have to go back and tell him that. But if you have that in front of you, the purpose of this is to clear up the misinformation about the National Security Decision Directive, '84, signed by President Reagan on March 11, 1983. Does everybody know the answer to number 1? First of all, the Directive is not an amendment to the Executive Order. The Directive is an effort by the Chief Executive to control a problem that every Chief Executive has complained about as long as I've been around, and that's the problem of leaks. NSDD 1984 primarily concerns leaks. But it doesn't amend 12356 to attack leaks. It simply augments, in certain respects, the particulars of the safeguarding foundation layed out in Executive Order 12356-just as they were safeguarding procedures in prior Executive Orders.

Britt kind of broke the Directive down into five parts. I think it's easier to comprehend it in three parts. Let's see if we can do that. The Directive is an attempt to control leaks. One by a dose of preventive medicine and second of all a dose of cure when there is a leak. And thirdly, addressing the problem of the personnel security system. You probably could throw number 3 over into number 1, but if we clean-up the personnel security system we'll help a little bit in the preventive medicine area. By preventive medicine, the Directive is concerned with putting people on notice about their obligations in dealing with classified information. It puts these people on notice by making them sign nondisclosure agreements. Everyone who has access to classified material — whether you're a government employee or a contractor — will ultimately be required to sign a nondisclosure agreement that meets at least the minimal standards of this National Security Directive. Now there are some distinctions to be drawn.

In the current drafting stage there are two nondisclosure agreements that we're producing. The first, the one that's gotten most of the press play, is the one that deals with persons that have access to Sensitive Compartment Information (SCI). Sensitive Compartment Information, you may be aware, is kind of an umbrella term for certain special access programs run by or through the Director of Central Intelligence to deal with subjects of intelligence sources or methods. SCI is not the only special access program there is in government, but it is the only special access program that the Directive specifically addresses. So all other special access programs will fall within the realm, at least as far as the Directive is concerned, of access to other classified information. The Directive's intent is to establish minimal safeguarding standards on a government-wide basis. This is so that each agency would have the opportunity to apply more stringent safeguarding procedures for programs that are particular to his or her particular agency or for certain aspects of a program within a particular agency.

Prepublication review is a requirement only in the SCI nondisclosure agreement. Prepublication review is, if you're going to write something, whether you're working for the government or contractor now or later and technically up to the day you die, and beyond. If you have an estate that wants to publish something, you have to submit it to the agency that last granted you a clearance. There's some concern over trying to get that with some precision in these nondisclosure agreements, because some people get lots of clearances from lots of agencies. We're trying to get it straightened out as to what agency you should submit it to. But, in effect, that agency will either review the material itself or will farm it out to agencies with subject matter expertise in order for them to review material and decide whether it contains any SCI or other classified information. They will take out or order you to take out any classified information. The form we are presently drafting for collateral information (information that is not SCI), does not contain any requirement for prepublication review. That

doesn't mean that an agency head could not have established such a requirement.

The polygraph aspect of NSDD84 is a very limited one. It has nothing to do with you getting a clearance. So when Britt talked about the experiment in Great Britain concerning clearances, NSDD84, at least, has nothing to do with using the polygraph for granting clearances. That doesn't mean that there may not be some agencies within our government (I think there are) that employ polygraphs because of their sensitivity. Unless an agency has a specific program, NSDD84 is not going to require any use of the polygraph for clearances. Polygraphs will only be used in the course of investigations when there is some indication that someone may be culpable and the polygraph is used in addition to other investigative techniques in order to try to determine who leaked information. Of course, another area that's very controversial in dealing with the polygraph is the fact that they have changed it so that if you refuse to cooperate in taking a polygraph when there's good cause, you can be disciplined up to and including being removed from your position.

Let's see which of these things I haven't answered yet. I think I've answered all but number 9, number 10, and number 12, if I'm not mistaken. If you didn't hear me say true and false, well so far it's true, false, true, true, true, false, false, true, and number 9 (the news media aspect of the Directive) has also gotten a lot of press play. Obviously, you say you'll take care to make sure that you guard against leaks to the news media; the news media are going to play it up very big because they view it as a contest. It's their job to get the information out of you and they don't want the odds stacked too highly against them. Nevertheless, most agencies even now have policies in place that probably would take care of much of this. The fact that you have to report your contacts, your news media contacts, or perhaps that two people have to be involved when you're discussing programs that may involve classified information. NSDD84 is not yet implemented. It's in the process of being implemented and, hopefully, it will be in the not too distant future. Again, you won't hear any bang. You'll hear far less of a noise even when 12356 went into place. Just about everyone who's going to be required to sign a nondisclosure agreement form already signed a nondisclosure agreement form. In time, it will just be a little different form with really little change in what your obligations are. Those of you who have contact with the media will be controlled and will be subject to controls that you're probably aleady under. The instances of the use of the polygraph, at least I would certainly hope, will be very rare. The one major change that will truly be a great and lasting benefit in this problem will be the President's expremiture in the idea of replacing Executive Order 10450. The answer to number 12 is false because the Directive did not come complete with its own new personnel security system. It only said let's create a new personnel security system. Incidentally, the document on the back of the quiz is NSDD84. It's not identified as such because, believe it or not, when the White House sent it out it was their decision that wouldn't identify it as such-even though that's what they said it was. You might want to ask me a question about that but I'm going to have a hard time giving you a very good answer. I know we're running behind here so rather than go on about 12356 or NSDD84, if any of you have any questions I'd be happy to try to respond to them.

Q: Al Baker, Georgia Tech. My question has to do with who is going to keep these NDI's. Has that been determined yet? The agency or contractors?

A: The nondisclosure agreements? O.K. What we're doing is creating two standard forms. They will be distributed to the agencies. They will be able to order them just like they can order any other standard forms in government. They'll have to stock them up and use them as their demand requires. One of the things that Britt said that I may disagree with him on, that DOD plans on implementing this thing entirely prospectively. I assume when he said that he means both the collateral form and the SCI form. The decision that's going to come out of the National Security Council is that in order to implement the SCI form prospectively you have to demonstrate that the current form you are using meets all the minimal standards established in the standard form that we're creating. Plus, there's an administrative burden in getting the thing signed by everyone. Obviously, DOD is going to have an administrative burden in getting even the SCI form signed

by everyone who has an SCI clearance in industry and in the Department of Defense. But I think there is some question among some agencies whether or not the current DOD form will meet those minimal standards. If that decision is that is does not meet those minimal standards, they'll have to be a period of time established for which DOD will be expected to get all of its employees signed up on the new form. That will include industry as well.

Q: Alan Thompson from the National Archives. Steve, a year ago you were talking about one of your programs, ISOO programs, to develop and to promogate new standard forms in a variety of areas. Could you tell us how you're making out in that?

A: Well, we were making pretty good progress. When the Directive came out we had an interagency group that already selected several forms including cover sheets for standardization. We were making alot of progress and low and behold the Directive was signed and our interagency working group was immediately taken off of any work of these other forms and put on these nondisclosure forms. Obviously, they take priority. Until we get those things resolved all work on the other forms has really halted, it's been postponed. I do expect that before the end of the summer we'll be finished with our work on these nondisclosure agreement forms and we'll be able to address again such forms and cover sheets which we do intend to standardize.

Q: My name is Ed DeMatti. I'm with Martin Marietta in Denver. You mentioned earlier about a waiver on portion markings for the new Executive Order. What are some of the guidelines on this. I know it's normally just the user agencies that go about submitting the waivers. What are some of the guidelines that justifies a waiver on portion marking?

A: The guidelines are in ISOO Directive number 1 and, regrettably, I didn't bring ISSO Directive number 1 with me up to the podium or even to Fort Worth. I can tell you the gist of those guidelines. We believe that there was a legitimate gripe about portion marking costing the government more than it benefitted the government. These cases were usually in those agencies where information was very tightly held and the information was not used in the derivative classification process. In other words, one of the things people have said in the past is that if you portion mark, and then you get an access request, you already have done your work. Well that wasn't the case. Obviously, if you get an access FOI request for information, even if you portion mark it, they're gonna rereview it. And so portion marking really wasn't assisting in that area. Where it really was assisting was in the derivative classification process. So many times you'll get in these huge documents that are not portion marked and you'll read so much trivial information that can't be classified. And, in some cases, your agency's kind of handcuffed if the information is classified. There's an absolute need for portion marking. It is in that area that we're very much concerned that portion marking continue. Wherever information is not closely held, wherever information may be used in the derivative process. I think the waivers that have been granted so far have addressed that rather fairly. Those waivers that come out of the National Security Council, out of the Department of State, out of the CIA, and, I think, out of one other agency. The traditional one was the Navy Atomic Reactive Nuclear Propulsion Program- right. In any event, those waivers look good or seem to look good on paper. What does not always look good is what's happening in practice. For example, the National Security Council which we have to hold up as a model and where the program comes from, has been guilty of a number of instances where information has been used, has been distributed to other agencies and the information's not portion marked based on the waiver side by Judge Clark. I know in that particular case that Judge Clark actually brought it up at one of the senior staff meetings that his employees and his senior staff were abusing that waiver. Hopefully, other agencies will do the same thing. It may seem that the agencies doing it are in the intelligence area where they may be dealing more with SCI, but the Department of State has relatively little SCI and very little intelligence information. The State is issued a waiver. Any other questions? O.K. Well then, thank you very much.

## THE ISOO QUIZ ON NATIONAL SECURITY DECISION DIRECTIVE 84

### TRUE OR FALSE?

Ⓣ F 1. The President issued NSDD-84 in March 1983.

T Ⓕ 2. NSDD-84 is an amendment to Executive Order 12356.

Ⓣ F 3. NSDD-84 primarily concerns "leaks" of classified information.

Ⓣ F 4. NSDD-84 applies to government contractors as well as employees.

Ⓣ F 5. NSDD-84 requires that all persons who are cleared for access to classified information sign nondisclosure agreements.

T Ⓕ 6. NSDD-84 requires that all persons who are cleared for access to classified information submit all their articles, books, etc., for prepublication review.

T Ⓕ 7. NSDD-84 requires that all persons who are cleared for access to classified information submit, if requested, to a polygraph examination in order to receive their clearance.

Ⓣ F 8. NSDD-84 specifically addresses Sensitive Compartmented Information (SCI), which is a Special Access Program established by the Director of Central Intelligence.

Ⓣ F 9. NSDD-84 specifically addresses contacts with the news media as an area that requires special attention in protecting classified information.

Ⓣ F 10. NSDD-84 requires agencies to report unauthorized disclosures to the Department of Justice, the Information Security Oversight Office, and the National Security Council.

Ⓣ F 11. A cleared employee who refuses to submit to a polygraph examination during a "leak" investigation may be removed from office.

T Ⓕ 12. NSDD-84 also introduced a new personnel security program to replace Executive Order 10450.

*DISCO CLEARANCE PROCEDURES*

**Gerry Crane**
**Chief, Personnel Clearance Branch**
**DISCO**

My objective this afternoon is to provide an overview of the DISCO operation and give insight into some of these activities involved in the Defense Industrial Security Clearance Program. So with that end in mind let me begin at DISCO's beginning.

In 1965, the consolidation of 115 Army, Navy, and Air Force personnel security clearance activities culminated in the birth of DISCO which was the field extension of Headquarters Defense Logistics Agency. Then in October of 1980, DISCO was transferred to the Defense Investigative Service as part of the merger of the Defense Industrial Security Program with DIS. Since our inception we've physically been located as the tenant activity in a secure environment at the Defense Construction Supply Center. DISCO was responsible for determining the eligibility of U.S. contractor personnel for access to foreign or domestic classified information or material, for processing visits of U.S contractor personnel to foreign governments, NATO and other overseas activities, and for maintaining automated records of facilities and personnel security clearances involved in the Defense Security Program. As indicated by Dick Williams earlier today, DISCO reports to Dan Dinan, the Deputy Director for Industrial Security. We also have a very close working relationship with the Office of Industrial Security International in Brussels; with the Defense Industrial Institute in Richmond, Virginia; and with the eight region Cognizant Security Offices in carrying out our mutual industrial security responsibilities. As you would expect, we have a very close working relationship with the Personnel Investigation Center in Baltimore. Finally, our association with the Defense Construction Supply Center is one of tenant and host. We rely very heavily on the center for mission-oriented and administrative-type support. DISCO operates within a very sophisticated computer environment. Our system was designed by the DLA Systems Automation Center and they continue to maintain that system for us. It is a real time system using teleprocessing via cathode ray tubes. Since our conversion to this system a number of innovations have been added to further sophisticate the system. For example, letters of consent and other correspondence are now computer-generated in a realtime basis. Contractors are being notified of personnel security questionnaire deficiencies by pre-designed computer-generated messages sent via autodin. Individual clearance records are being automatically updated by the computer as favorable national agency check results electronically transmitted to us from the Personnel Investigation Center in Baltimore. Our automated records consist of the facility address file, the personnel security clearance file, and the unprocessed file. These files are accessed as one central file. Any record can be immediately updated or reviewed simply by calling up that record using one of 22 CRT's located throughout DISCO. At the head of DISCO, of course, is Lt. Colonel Eric Holt. I am working with him as the acting Deputy Director during the temporary absence of Mr. Mead who is ill and convalescing at the moment. Also, working with us in the Office of the Director are two secretarial staff members and two staff coordinators. The Privacy and Freedom of Information Coordinator has the added responsibility of coordinating all cases with high level congressional or presidential interest. MODISCO was an acronym informed mechanization of DISCO. Our MODISCO coordinator has the responsibility of the development, administration and coordination of DISCO's ADP systems. The Operations and Analyses Office performs operational reviews to assure that DISCO is functioning both efficiently and effectively and also monitors our manpower, financial management, and quality assurance programs. The Personnel Operations Office reports to the Assistant Director of Personnel and Security at headquarters, and handles all of the personnel management matters for the civilian employees at DISCO. The current support division consists of the input-output control branch and the clearance records management branch. The input-output control branch process all incoming and outgoing mail to DISCO and they also initially build clearance applications into our Personnel Security Clearance file by means of the cathode-ray tube. This branch also is responsible for the distribution of all automated data processing print-outs such as letters of consent, and automated letter messages. The Clearance Records Management

Branch is responsible for overseeing the maintenance of our pending and closed clearance page folders. Another function of this branch is to maintain our status inquiry desk to respond to requests from contractors and user agencies concerning the status of a particular applicant. This desk has direct on-line access to the MODISCO system. This, then, enables the DISCO status clerk to immediately ascertain the status of a particular case by querying the in-process file record. Incidentally, DISCO has a 24 hour telephone answering service. Our telephone number is 614-236-2058. You can call that number at any time. We'll relay the information that you'd like to have from DISCO. Usually the next working day a member of DISCO will call you back with the proper response. The Personnel Clearance Division is the largest division in DISCO and is composed of four branches. The Initiation Branch screens all personnel security questionnaires to insure that the minimum data necessary to initiate the request for investigation is contained on the form. If the form is complete, as it name implies, they will initiate the request for investigation by submitting the documents to the Personnel Investigation Center. However, if the form is found to be deficient, that is it is lacking some information critical to the investigation, the Initiation Branch will so notify the contractor either by autoden message or by letter. This leads me to a very important subject and that is Personal Security Questionnaire Rejects. When you consider that the average PSQ reject will delay clearance processing by approximately five to thirty days, the reason for our concern becomes clear. We're very pleased with the fact that we have driven our reject rate down from FY81 (when it was 14%) to our current rate of 6.8%. However, I must be candid with you. For the last three months we have noticed a most unfavorable trend developing. The reject rate had been inching its way forward. It is our belief that this increase is due to the new DD forms 48 and 49 and once industry becomes acclimated to using the new forms we will once again see a reduction in the reject rate. I would like to echo something again that Dick Williams said, and that is the use of the new DD forms 48 and 49 certainly will reduce the overrall processing time not only for contractors but also for DISCO. Looking at the major deficiency reasons you'll note that the Privacy portion accounts for almost 60% of all the rejects. Let me acknowledge that it is that portion generally to which contractors do not have access. I submit to you that those members of industry who are here today should spend a few moments with the applicant and review the Privacy portion, and concentrate particularly on three data elements. The arrest details, medical data, and currently the organizational membership block on the new 48-49. Interestingly enough, we've been finding more and more of the items 16B1 and 2 on the 48 or item 19B1 and 2 on the 49 because the individual is not completing one of those two blocks. With respect to part one, there is no one particular item that has generated the greatest number of deficiencies. I would suggest that before you submit the form to DISCO you review particularly four data elements, i.e., relatives, employment data, residences, and foreign travel, to assure that it contains all the data that we need. There are two rejects that, frankly, I find rather confusing. One is fingerprint cards. The reason for that is there has been so much publication, and so much advertisement about the FBI ruling that says they will not accept any fingerprint card unless it's an FB258 addition dated April 25, 1972, or later, or another commercially produced fingerprint card approved by the FBI. Not withstanding that fact month after month we continue to see 10, 11, 12, 13, 14% of all the applications with the old fingerprint cards. Frankly, I don't know where they're coming from. I really don't care what industry does with them but my recommendation is please don't send them to DISCO. We cannot accept them. We have to send them back. As a matter of fact, let me make a suggestion to you. When you go back to your respective companies check your stock of fingerprint cards, and if they're not an FD258 of April 25, 1972, or later, or another commercially approved fingerprint card by the FBI, do not use them for the Defense Industrial Security Clearance Program. Regarding the required documentation, DISCO does not reject for an absence of an SF50 or a DD214; or we certainly rarely reject for them. The 15% relates to an absence of the DD2221. What is mind boggling to me is that on the new DD form 49, the first page, section 2, is the 2221. Twenty-eight percent of all the new 49's we receive will not have the 2221 there. I really don't know what the applicants are doing with them, but they're keeping them. We really need them so, again, I would suggest to the representatives of industry here today, would you remind

the applicants when you give them the Privacy portion to complete to please send the 2221 to DISCO. Two additional items on the rejects and I'll get off my soap box. One is that we're receiving about 25% of our applications minus the facility code. That five digit code or five character code is extremely important to the DISCO process. If you do not have it on the form, we can obtain it. We do it through an automated search which is certainly a lot faster than when we used to have to search under a manual system. To let me give you some idea of how much you're delaying the clearance process, I can build three in process records in the same length of time that it takes to find the facility code number through our automated search. On the new DD form 48 and 49 there is a block provided for the facility code. Twenty percent of the new forms that are coming in have that block left blank. One additional item is verification of citizenship. We do not withhold the initiation of the investigation for that data. We will certainly put the investigation in process, but we're not going to grant the clearance until we receive the information. To give you some idea of the volume of requests coming in minus that information, or minus the statement that the contractor is attempting to get the form, 830 applications last month did not have this information present. So again, to the representatives of industry here today, if you could address your attention to the items of the PSQ and related documention that I addressed you can greatly facilitate the processing of clearances. The bottom line is that your going to allow DISCO to get you the clearances granted faster. The Initial Clearance Branch processes the bulk of DISCO's clearance determinations by granting clearances to persons on whom only favorable or clearly minor unfavorable information has been developed. Any case which is found to contain major derogatory information is referred to the Adjudication Division for review and analysis by our senior professional staff. This branch also processes interim clearances and all foreign travel reports. The Clearance Update Branch processes conversions of former military and civilian personnel clearances to an industrial type. They process transfers of clearance from one contractor to another. They post changes to the Personnel Security File as reported by contractors. Some examples are: terminations of employment, reinstatements, name changes, citizenship changes, reports of overseas assignments, etc. The Priority Programs Branch has a multiple function. One of which is to maintain accurate, automated records on over 12,000 contractors actively participating in the Defense Investigative Security Program. They process visits of U.S. contractor and foreign personnel to contractor and other activities. They also monitor or control all NATO reciprocal changes as well as furnishing U.S. security assurances to foreign governments. There's another way in which contractors can help DISCO grant clearance faster and, ironically enough, that's by reporting terminations. The faster DISCO receives information concerning a person who either already has been granted clearance or is in the process of being granted clearance, the faster we can get our data records corrected. This is especially true for contractors who are in process for a clearance. As soon as we receive the information from industry that this person has either terminated employment or no longer needs the clearance, we immediately convey that information to the Personnel Investigation Center to stop unnecessary investigations. The bottom line is that we are allowing the DIS field investigators to beat the bricks of those people who need access to classified information, rather than expending their efforts on those people who are really no longer involved in the program. The Adjudication Division, as I said earlier, processes all cases containing significant derogatory information. Or, to put it another way, those cases that are judged to be more than just minor. What do I mean by minor? Some examples have popped to my mind immediately-traffic violations. Purely minor offenses while in military service-failure to salute, missing revelee, smoking in a no smoking area. Violations of game laws-fishing without a license, bagging over the limits. The primary adjudication of cases is accomplished by personnel security specialists called Primary Adjudicators. A second independent review and opinion on these cases is furnished by a higher grade of specialists called Senior Adjudicators. This division also coordinates all special access program cases such as sensitive compartmented information, and presidential support activities, which is certainly the most active program at DISCO today, the Circle A program. Finally, this division also processes all adverse information reports received from industry, under paragraph 6B1 of the ISM, this cleverly leads me to the next topic, and that is

adverse information reports. I hesitate to say too much about this because I don't want to beat it to death. However, DISCO does take advantage of every opportunity to emphasis how important it is to us that adverse information reports be submitted to us on an expedited basis. This is so that we make an immediate judgement concerning the individual's continued eligibility for a clearance. It's evident from the data reflected in 1982 that our efforts have certainly not been in vain. More adverse information reports were received in FY82 than in any other year in our history. For the first eight months of this fiscal year we have almost surpassed FY82. There's no doubt in my mind that we will receive at least a thousand 6B1 reports this year alone. But let's be honest with each other. Considering that there are 12,000 contractors participating in the DIS and between 1.2 and 1.3 million contractor personnel that hold a clearance, I submit to you that that is the tip of the iceberg. I have heard some persons suggest, "Oh, there's really not much sense in sending the information to DISCO. They really don't do anything with it anyway." Well, let me quickly dispell that myth. Indeed we do act upon information and we do so quickly. If DISCO receives information about someone who already has a clearance, we feel the information is so significant that interim action is warranted in the National interest. A recommendation is submitted to headquarters DIS to suspend the individual's clearance. Final decisions in these cases rests exclusively with Mr. O'Brien as the Director of DIS. We have had more interim suspensions affected and in process this fiscal year than we have ever had before. And again, this relates directly to the number of adverse information reports that we are receiving. We cannot act on the information unless we received it. Very often contractors will not know that DISCO is taking some action on the adverse information report because we do not always ask for new personnel security questionnaries. As a matter of fact, it's the exception rather than the rule that we will ask for new personnel security questionnaires because of some adverse information. We have the capability within the DIS family to have an investigation conducted based upon the information as furnished to us. I'm not saying we never ask for personnel security questionnaires under these circumstances, but I say to you that is the exception rather than the rule. In processing new clearance requests, if DISCO feels that we are unable to reach a favorable conclusion, and we feel that the issuance of the clearance is not clearly consistent with the National interest, then the case is forwarded to the Director of Industrial Security Clearance Review (DISCR) within the Office of General Counsel at the Pentagon. The DOD directive which governs the Defense Industrial Security Clearance Program identifies 14 separate criteria to be used in determining an individual's eligibility for a security clearance. Marijuana, alcohol and hard drug abuse account for 60% of all of our referrals to DISCR. I might add that those three factors have been the dominant factors for several years now — with the other criteria coming in for smaller slices of the pie. I would like to review with you some current statistical data about DISCO's average monthly workload. DISCO's input in all of our major function areas has been increasing and in some cases, substantially so. There's really only one minus sign and that is cases in process. That's a positive indicator for the investigative side of DIS. The less cases that we have in process is an indication that the Personnel Investigation Center and the field investigators are closing the investigations to DISCO much faster. In FY82, DISCO received more new clearance requests than in the last seven years. When you consider that the majority of DISCO's man hours are consumed in processing new clearance requests, the significance in the continuing increase of that data element becomes obvious. Even though DISCO was receiving more and more requests for clearance, which translates to request for investigations to pick, the Personnel Investigation Center and our investigators are still closing the investigations back to us much faster. The DISCO clock begins at our mail room, where all clearance applications are date and time stamped. It's at this date that DISCO effectiveness is measured. That clock continues to tick over weekends and holidays, and it includes unforeseen work stoppages such as a power failure and computer down time. When under DISCO's control, the turner on-time is respectable as evidenced by the interim secret and transferring concurrent times. The processing time of new secret clearances on beginning with those based on an autonac which is an acronym for Automated National Agency Check is the fastest means by which a new secret clearance can be granted. To those issued by the Adjudication Division, the

more time-consuming of our in-house processing times, the Autonac system enables DISCO to open certain types of NACS by actually sending the lead request directly to the FBI via express mail. The Bureau will check the lead and send the results to the Personnel Investigation Center. If favorable, PIC will electronically send that NAC result to DISCO. As a follow-up to that system, our computer intercepts that electronic NAC transmission, posts the individual clearance record, and upon direction from a DISCO representative (usually the first thing the next work morning) will produce that letter of consent on a printer located in DISCO without human hands ever touching that case folder. As you would expect, those cases which involve adverse information are more complex and require additional handling to process. The amount of time involved in issuing the secret clearance rises accordingly. But what is significant is that 65% of all of the secret clearances that we issue are granted faster than the so-called average of 73 days. You must remember that average is an arithmetic mean and is a blend of all the categories of processing. The processing of special access programs has had a most dramatic impact upon the processing of top secret clearances. Particularly, most of the special access programs require the conduct of a special background investigation which is more time consuming than what is normally required for the collateral DOD clearance (the Interview-oriented Background Investigation). Nonetheless, with the added resources allocated to the DIS investigators, we are seeing a steady compression in the amount of time that it's taking for DIS to complete investigations. Of course, that allows DISCO to grant top secret clearances faster. Mr. O'Brien talked earlier today about the Defense Investigative Service, the investigative side, and reducing the amount of time it takes them to process investigations. Let's look at the backlog of DISCO cases pending at the Personnel Investigative Center (PIC). I'm talking about all types, not only the personnel security investigations but also the NACs. In May of 1981, PIC had 38,700 DISCO investigations pending. Two years later, in May of 1983, they had reduced that backlog to 26,600 cases, a reduction of over 12,000 cases. Remember we are putting more new requests for investigation into PIC now than we have ever put in before. Nonetheless, we are seeing a compression in our processing times. I was looking at the amount of time it was taking DISCO to grant TS clearances at the beginning of FY82. I'm talking about cases absolutely void of adverse information — absolutely clean. At the beginning of FY82 it was over 200 days. At the beginning of FY83 it was 149 days. Today our average time is at 111 days. If you look at just the clean cases, which again accounts for over 50% of all the TS clearances, our average is at 81 days. Don't misunderstand me. I'm very pleased with that. But I'm certainly not happy with it. I'm not going to say that we're going to rest on our laurels. We've got a long way to go before DISCO's ever going to be satisfied with that. But we are making progress and we will do better.

My final topic is periodic reinvestigations. I won't go into as much detail as I had planned to since several people have already eluded to this. Basically, the Periodic Reinvestigation Program applies to all persons who have a top secret clearance, have access to single integrated operational plan (especially sensitive information), hold positions as COMSEC facility security supervisors, custodians or alternate custodians or have access to sensitive compartmented information. For our purposes, DISCO controls the request for PSQ's for three categories: top secret, SIOP and COMSEC. We will notify the contractor when we require the PSQ for the Periodic Reinvestigation. The SCI component will notify the contractor when PSQ's are needed for the SCI access. Those forms are ultimately sent to DISCO. DISCO has the overall responsibility of controlling the quota that Mr. O'Brien spoke about earlier. When DISCO identifies the need for a periodic reinvestigation we send the contractor a letter notifying you of that requirement. If we don't receive a response within 30 days, we send you a tracer that we still haven't received the form. Thirty days after that, we send you a letter telling you that if we don't receive the PSQ's or a response we'll assume that you no longer need the clearance and we'll institute action to administratively terminate the clearance. There are 75 days involved in this process which is ample time to get the forms to DISCO or notify us that the person is out of the U.S. or is having difficulty getting the forms together. I can understand that and I'll tell you why in a minute. Nonetheless, if we receive the information we'll hold the case open for you for a reasonable period of time. If we do not receive the forms we cannot

hold these cases open infinitely. There will come a period of time where we will, in fact, administratively terminate the clearance. In January, when I had volunteered to be a member of the Periodic Reinvestigative Committee, I decided I had best find out about how many cases that we were talking about. I said, "Ms. Computer, tell me how many contractor personnel we have in our data base with an active TS clearance based on an active intestigation more than five years old?" It comes back the astounding statistic, 45,601. That represents 47% of all of the active TS clearances in our data base. With that information I said, "Tell me, Ms. Computer, how many TS clearances are based on an investigation more than 15 years old?" It comes back to me 14,453, or 32% all people that have a TS clearance that need a periodic reinvestigation. You want to know how old some of these are? I drew my first listing of 1,500 names since I obviously can't work with 14,000 names. I drew 1,500 names at a time. The last name on the first listing had a date of investigation of September 17, 1954. I recently drew my second automated listing or the 3000th name (that's hard for me to say). We're making progress. The last name on that list had a date of investigation of Decemeber 24, 1958. We're now only 25 years old. Bear in mind these people are continuing to have access. Think how old all those investigations are. When DISCO receives a PSQ's, of course they're all going to be properly completed, we will naturally request the request for Periodic Reinvestigation through PIC. When the results come back to us they're evaluated in the normal manner. Those that are clean or contain minor information will be cleaned out and processed by the Personnel Clearance Division and those that contain derogatory information will end up in the Adjudication Division. If the decision at DISCO is favorable to the applicant, the contractor will be provided an automated letter message telling you that the investigation has been updated. It's the system that we've used for sometime with special access programs and the old COMSEC procedure so we're going to do the same thing for periodic reinvestigations. If the decision is unfavorable to the applicant, and I reiterate here that these decisions are rendered by the Director of Industrial Security Clearance Review at the Pentagon, not by DISCO, the contractor is notified by DISCO, by letter that the individual's clearance has been revoked by DISCR, and will be directed to take immediate action to prevent the individual from gaining further access to classified information. The bottom line here, ladies and gentlemen, is that the success of the PR program rests in large measure squarely on the shoulders of the contractors. Mr. O'Brien talked about the Periodic Reinvestigation Program and the investigative workload at the Defense Investigative Service. We can absorb the Periodic Reinvestigation Process, providing it's done in a timely manner. DISCO controls the quota and that quota varies from month to month. I really don't know from month to month what the quota is going to be until after the Personnel Investigation Center makes a judgement concerning its workload and what the workload is at the various field activities. DISCO will try to forecast at least 90-120 days in advance what our requirements will be for the Periodic Reinvestigation process. Unless we receive these personnel security questionnaires back from you, our ability to respond to that quota will not be possible. As I've been talking I've been reflecting upon the progress made at DISCO and I smile and think "is it any wonder that I look to the future with great anticipation of what is yet to come?" Our limitations are really not there. The horizon is unlimited in this day of the computer and electronic communication between long distances progress. We haven't begun to fight. We haven't begun to start. I want to thank you for giving me the opportunity to share with you some information about an organization which you may have guessed I am quite proud. And for myself, may I say, that I truly consider it quite a privilege to have been asked to address such a distinguished audience. You've been most kind. Thank you.

Q: I would really like to commend you for the courtesy and the helpfulness of all the staff at DISCO. Everytime I have called, and I know sometimes I've made a pest of myself, they are very patient and very helpful. And that's in every division. The only difficulty I've ever encountered is finding the right person to answer my question. They aren't ready to transfer my calls, but I asked if there were a directory. I've made my own little list of which extension to call for which question, but this is changing all the time. They sent me what they had. I was wondering if it wouldn't be possible to publish a little directory.

A: That should be food for thought. We may be able to include something in one of the Industrial Security Letters indicating if you have a question on conversions call a certain number. That's a very good idea. Thank you.

Q: My name is Bob Keller. I'm from Watkins Johnson Co. in California. My question is concerning why it takes so long for a name change to take effect and get an LOC out for it. I submitted two name changes for two ladies that got married. I submitted them a month ago and I have not heard anything from DISCO, whatsoever. I have sent out an inquiry like I do every month for all my clearances and all I got back is that it was pending. I called DISCO and the lady I talked to (I might say that it took me four hours to get through) says, "Oh, our computer is down." I can understand that. I said, "Well can you take my name and the persons' names that I want to try to find out about and get back to me?" she stated, "I'm sorry but I can't take your name and get back to you. We don't make phone calls."

A: I'm glad you brought that up. If I'm assuming that you called 2265-that's the General Status Inquiry Desk.

Q: All I remember is the last four digits were 2500, I believe.

A: 2500. I'll kill her. No I'm not. Obviously, that was not correct. I don't care who you call in DISCO if you've been on the phone for a long time or if a person's been transfered more than twice, that is our limit. The person should not be transfered more than twice. That's the bottom-line. That's the procedure at DISCO. Yes, I see the fingers here, but I'm telling you that should not occur. This is the kind of input that I need. I'm sitting back in my office thinking, 'Boy, aren't we doing great work? Everybody in industry is happy. DISCO's doing what we should be doing. That's the kind of input I need. It will give me the feedback that I need to go out to our personnel and say, 'Whoever's on extension 2500 or 2265, remember this is our policy. These are our procedures. You will not refer that contractor two, three or four times. You take the name and telephone number and then every supervisor is admonished to assure when you make that call you're given a response. That goes for everybody in this room, user agencies, Cognizant Security Offices, contractors, whoever calls. No matter what your question happens to be, you are entitled to a response. If we tell you we are going to get back to you today, even if we don't have the right answer, we owe you a return phone call. Now to get back to your basic issue on name changes, a name change should never take more than 10 days maximum in-house. It is purely a paper change. To do a header-data change requires about 30 seconds. So if you have those two names, jot them down for me. Or, I'm on extension 2133 and I'll be back at work Friday. Give me a call and I'll find out. That's the kind of thing that I'm concerned about. If anybody else has those kinds of problems, I truly do need to know about it. 2133. Watch me get inundated with phone calls, but that's OK.

Q: Pam Hart, ALM, Inc., Arlington, Virginia Do you have a time limitation for at least notifying the contractor that you might be having some kind of problem with the clearance?

A: No.

Q: So you're just not going to tell us?

A: Right.

Q: It's just going to be an indefinite thing.

A: Right.

Q: And that's it?

A: Right.

Good-bye. I want to thank you all very much. You have all been very gracious. Thank You.

## *DIS WORKSHOP*
## *MARKING REQUIREMENTS*

**Sheila Daigle**
**Defense Investigative Service**
**San Francisco, California**

I am going to take a different approach. I want this to be an informal workshop and I do want questions.

We have gone over your page markings, overall markings, subparagraph markings, and things of this nature. I am going to start this morning with some of the other markings that go on documents -- markings that could be used in certain instances, because I find that we have not touched that much on it in some of the workshops that I have participated in. A set of Marking Requirements have been given out. (See handout pages 48 thru 56) The first session this morning will be on the classification pending marking. I have been getting a lot of questions in my office about this marking-when you use it; how do you use it; what do you do after you've applied it? I have found that there are many instances where you need to know how to apply this classification pending marking, and when and how it should be used. It should be used with great caution. It should not just be used because you do not know what else to do. There should be a bonified reason for it. You use this marking when you have material that is strictly unassociated with a program or project that has a current classification guide assigned to it. It would be material that is very similar to the field of interest that is used by your company or your user agency. Both would have had past experience in where that material has been classified at the Confidential, Secret or Top Secret level. The brand new material which you are developing (usually in an R and D effort) would normally be proprietary to the company. You would mark it with the classification determination pending marking, and you would insert the level that you feel is applicable to that particular material. You could add, if it's in a company situation, the statement that this is company private or proprietary in addition to the classification pending marking. The one catch is that when a company has done this, they would have to send the material to that government activity that they had been doing work with in a like situation or a similar field of interest. For the government's side of the house, you would want to send it through your chain of command to your classification authority.

There are agencies listed in the Industrial Security Manual which will tell you who you could send the material to if you are in doubt. If you say "I am not working for anyone whatsoever," then you would send that material to those agencies that are listed on page 252 or 253 of the Industrial Security Manual. The distribution of this document should be limited so that you will be able to track it back when you receive your classification determination. You are to receive a classification determination within 30 days from the time you send the material in. Now you will not find that in the Industrial Security Manual because I looked for it very thoroughly. I don't know if you will find it in some of your other government regulations that you are working with. The Executive Order does state when you send material in for a classification determination, that the activity that you send it to has 30 days in which to respond. You should follow up. You should do everything you can to obtain that classification determination in a short period. Don't let it run for a year or two. You're only going to be creating more of a problem for yourself if you do that. If you don't receive, and this is on the facility side of the house, or industry I should say, then what you need to do is to come to your Cognizant Security (COG) Office and we'll do everything that we can to assist you. I am currently working two of those cases. We are making progress very slowly.

I have found that a user agency did come back to the contractor with the determination not quite within the time frame. That's all right. It came back. They had told the contractor to use the marking that this had been classified by the Patent Secrecy Order. Now this is not a correct classifying authority. If you receive something of that nature, do let us know, particularly in industry, and we will do what we can to get the problem reworked for you so that you do get the proper classification authority assigned to your material. Now that's sort of, in a nutshell, what I had to say about that. Does anyone have any questions?

Q: I'm Shirley Kostenbader from Northrop Corporation. What happens when you send something to an agency that you're working with and they make a determination that they do not want to tell you what the marking is because they're not going to give you an RFP, or such. This has been our answer to one of our problems that we had. They said they can classify it but they don't want to because they're not really that interested and that they don't plan to pursue that area. What do you do?

A: That's something I'd like to check into. However, my feeling would be that you would hold it as a company private or proprietary and come to us and see if we could be of any assistance and get it corrected for you — to get a definite decision, one way or another.

Q: In other words, if they don't classify it then it isn't?

A: That's right. The government has to show a proprietary interest in the information.

Q: And if they don't, then it isn't classified.

A: Now that's something that I would like to clarify. I think that's the basis that we would have to work on.

Q: My engineers tell me that from the field that they work in they feel that it's classified; and they feel that it's classified SECRET.

A: What justification was used in order to send the material back or to apply a classification pending marking? This is another thing that is very important. I neglected to say that when you are applying a classification pending marking to material and you're sending it forward, you should provide full justification as to why you feel that that material is classified. Maybe your justification was not strong enough or did not express what you were really trying to protect. But until a government activity authorizes the classification you cannot carry it as classified.

Hopefully, you'll be able to take these sets that I have worked out for you back to your activity or your facility and utilize them in some of the things that we do run into. I made a valiant attempt to condense the Industrial Security Manual as markings go down into six pages. You will find that there are some things that I do not mention and I have done that deliberately because I was not too sure that we would have the time to get through what I have here. I thought on the second set what we would do would be to talk about the additional markings or the special access markings (see enclosure pages 48 to 56). I elected to start out with the RESTRICTED DATA markings.

You do have to apply this marking whenever there is SECRET RESTRICTIVE DATA contained within the document. It only has to appear once. The total statement should appear on the front of the document and it must also show the classified byline. It does not have to show anything other than that. The same would apply for your FORMERLY RESTRICTED DATA marking.

Q: Elaine Gruber, System Development Corporation. I thought that the latest change of the ISM eliminated the classified byline on RESTRICTED DATA and the FORMERLY RESTRICTED DATA.

A: I did not think so. No. The same is applicable for your FORMERLY RESTRICTED DATA marking. I have given you in your sample what the full statement would be that you would apply to the front of the document. I will briefly go into the fact that your paragraphs have to be properly marked with the SRD but we'll get into that a little more downstream if we have the time. The WNINTEL notice—I have seen it spelled many ways. I am hoping that I have come up with the correct abbreviation of WNINTEL because I also have seen it as just WINTEL. But I think we have the correct one here. This is a marking that you would apply to material that contains intelligence information. It only has to be applied one time on the front of the cover, so far as the total statement goes. It would also be used when you have a classification guide that tells you that that material contains WNINTEL or you have a 254 that instructs you to apply that marking; or when you are extracting information from another document that carries that marking.

The other area that I have found that we have had some questions on is the Foreign Government Information marking, or FGI. You do use this marking on material that contains foreign government information and you are going to be using it to ensure that the information is not declassified prematurely or disclosed to a third country without the consent of the originating country.

Q: Junius Layson, the Boeing Company. Although the ISM doesn't specifically show it, we have chosen to put the OADR marking on the foreign material that we receive. In conjunction with the material that's being incorporated into

U.S. documentation, the ISM shows the marking, "this document contains NATO classified information." Or, the other one where it is not NATO, foreign government information. One of the problems we ran into is that if we mark foreign government information, people interpret it that's all there is to it. So we have chosen to use the same type of marking that there is for NATO, saying this document contains foreign government information.

A: But not using the NATO in addition to that? Just this document contains foreign government information.

Q: Yes. The second problem that we ran into is in many instances the U.S. information that's involved is not OADR. It has a specific downgrading or declassification data. So, we've found it necessary to have a bibliography in the document and the OADR overall marking because it's the most restrictive. But we're making an explanation that that applies to the foreign government information only. And the U.S. information is downgraded or declassified with whatever the particular instructions are for that. An additional problem that we've found is that in some instances, we have contracts where the U.S. information is classified at one level and that same counterpart information is classified at a different level but foreign government. We have inserted in our Standard Practice Procedure (SPP) a requirement in that instance on the paragraph markings that you show both classifications. For example, FRG SECRET, U.S. CONFIDENTIAL or U.S. UNCLASSIFIED, as the case may be. Otherwise, we've found when people are extracting information out of that, they would be applying an erroneous classification to it. Of course, if you get some information from foreign governments that they've had as UNCLASSIFIED or CONFIDENTIAL and you send it back to them SECRET they get a little upset. So, there are some areas like that that haven't been specifically covered in the ISM that if some of these people are dealing a lot with foreign governments they're going to find that situation. We have chosen wherever foreign government is incorporated in a U.S. document, that we not only mark all the paragraphs with the normal markings for U.S. information, but we specifically mark the foreign government information.

A: When you get into your paragraph marking you are to show the level, if I'm understanding what you're saying. You would show, for instance, SECRET and then Canada, U.K., or whatever the case may be. It sounds as if what you are doing there should be no objection. It may be over and above and that is perfectly all right. As long as the reader of the document knows what the classification is, in your instance the country, and there leaves no doubt in their mind, then I see nothing wrong with going over and above the requirements of the ISM. That's your company's choice to do that. Would you like to comment on that, Sandy? Yes, it is a lot of trouble but this way it certainly does not leave any doubt in anyone's mind as to what is classified and where it comes from.

We appreciate you doing all that extra work. Thank you very much.

The next thing I have discovered is that some people do not understand there are two types of NATO markings. You would use the statement, "This document contains NATO information on U.S. documents which contain extracts from NATO-marked documents. Then you would use NATO SECRET, NATO CONFIDENTIAL, NATO RESTRICTED, or the COSMIC TOP SECRET", as the case might be, on documents to signify that they are the property of NATO. There's kind of a distinction there, and that can be confusing.

Q: Liz Heinbuch, with Headquarters, Department of the Army. Why am I under the impression that you cannot put a NATO SECRET classification on a U.S. originated document? In the army we cannot do that. We only put SECRET. We cannot classify a U.S. originated document NATO.

A: You would not do it unless you had been designated to do so.

Q: By whom?

A: It would have to be the foreign country that you're dealing with. You do run into that sort of a situation. Well, not you, because you're a user agency.

Q: For the army or for the military, we could have a document that we originate as SECRET;

send it in to NATO; they would mark theirs NATO SECRET; we would hold ours as SECRET because we cannot stamp a U.S.-originated document with SECRET NATO, or whatever.

A: It is my understanding that we do not enter material into the NATO system at our level. It must go back through a channel for that marking. However, if, and I have run into this situation, it is a NATO contract and the contractor has been designated to mark material as NATO, then it is NATO property. Does that help any?

Q: I'd just like to comment on some of our experiences. The regulation says that if a country participating in NATO transmits documents to them, the NATO marking is applied by the last government agency handling it before it goes over. The NATO marking is applied once it goes into the NATO system. We have run into situations where we have the document that's U.S. marked, we retain copies of it, some copies are transmitted to NATO, and we can get the same document back through the NATO system that is now marked NATO information. We have two copies in our possession simultaneously. One with the original markings; the other with the NATO markings. Actually, this material doesn't become the property of NATO. It remains the property of the country of origin. But it is controlled in the NATO system with NATO markings. This is the interpretation that we've gotten back through our NATO channels. Does that help clarify?

The other day someone brought up a question on the CNWDI marking. This marking is applied to documentation that reveals a period of operation or design of components of a thermanuclear or implosion type fusion bomb warhead, demolition, munition or test device. You would also apply this marking when you have been told to by your classification guide or your 254, or when you're extracting the information from another document that carries that marking. You would apply it to the first page, cover sheet, and title page as it is shown on your sample guide. It would show Critical Nuclear Weapons Design Information, DOD directive 5210.2 applies. But it is only shown the one time in front of the document. I am not in a position to answer any questions on SIGMA categories. I just know that there are those. They would be applied only as you've been directed. Does anyone have any other questions at this particular time before we go on to the Classifying Authority?

All documentation that becomes classified must show a classified byline. That is a mandatory statement that must be applied to your documentation. I'm going to advise you, and I'm sure that this is going to come up for some discussion, that you would place the date of your 254 plus your contract number or the IFP, RFQ, or RFP number, whichever would be appropriate, or as designated you'd use whatever has been provided by your user agency. If they tell you to use an OPNAV instruction as a classifying authority, then that is what you'll want to use. If you're going to show the term Multiple Sources, along with that, because you have classified your document as a result of a series of documents in addition to information that you are working on the contract, you would add the term, And Multiple Sources. You will not show Multiple Sources standing alone. Now when you do use the Multiple Sources statement, you are going to maintain a record to support that statement and it must be retained for the duration of the contract or program for which the document has been created. My recommendation would be, and I do recommend it all the time, that you maintain it as a part of a bibliography type page to your document. You always will have it with that document. That way anyone who has that document may look at that bibliography and know why you classified, and under what authority.

Q: Because of these problems, our company has chosen to maintain the record of the document as long as there is a document in existance in the accountablity system. I know the requirement says you retain it for the duration of the contract or program, but you run into many situations where the document is originated on one contract or program that phases out. There are follow-on contracts and if you don't have a record of it, your going to find your material, that was originated under a closed contract, is eliminated after a certain portion of the time when it is already into the new contract or program.

A: That is why I recommend holding a bibliography with the document.

Q: Our position is as long as that document is in existance, there will be an explanatory bibliography somewhere in the record system.

A: Well, if you have the bibliography or the record with the document and I have the document in my hands, it is going to save me a lot of time and I don't have to come back to you and say, "how is this document still classified?" or "why did you classify it this way?" I can look right there and tell you, and tell myself.

Q: Catherine Allen, Northrup Corporation. This Multiple Source that you are talking about, is that extra, is that a direct extract from the Industrial Security Manual, or Executive Order, because we have used Multiple Sources standing alone on our documents and then included a bibliography of exactly where that source material has come from and where it was derived from. I don't recall where it says you can't use Multiple Sources standing alone.

A: One moment. Have you got that section? Pin point it. I have used the Industrial Security Manual, and I have used the 5200.1R to prepare these samples that I have put out for you. I am sure this is the term, the way I have it and it has come directly from the manual. If you will give us just a second, Mary Joe will look that up. Ok, on page 254 of the Industrial Security Manual you will see the exact words that I have here. Paragraph B2.

The classified byline would show the date or event that has been designated by your 254 or other classification guideline. You would use the most restrictive date of the source document material that you have incorporated, or you would use the originating agency's determination required (OADR) marking.

You would use the OADR if the 254 or the Source Material shows an indefinite date or event, a declassification review date, or no date or event for declassification.

You do not always have to use the marking downgrade to and on, unless you have been designated by your 254 to do so, or your other classification guideline, or if it shows that on your source document. If you are going to use it, then you would downgrade to "SECRET" or "CONFIDENTIAL" as the case may be, and you would indicate the date. That date would come from the documents that you are extracting from, or as you have been directed. I have shown you some samples here of the classified byline, the declassified on-line — how they could, and should look on your document.

Q: Elaine Gruber, SDC. We have made it a general practice at SDC to use the three line stamp because we figure sometime in the future it would be downgraded. We put N/A for "not applicable" if it isn't applicable at that time. You're not saying that it is wrong to do?

A: No. I'm not saying that. I am saying that you do not always have to apply that. But, to me it sounds like it would be alright. I would pass on it as your rep, let me put it that way.

Q: Ruth Jenson from Comtec Research in Buffalo. On the downgrading portion, if our documents show a contract number elsewhere on the title page, or front page, we do not have to repeat the contract number under the downgrading portion, do we?

A: I'm sorry you said that. I just had a very big argument with my husband on that point. Sandy, I'm going to bounce this question to you, if you don't mind, please. My response, by the way, has been *Yes*, you do have to show it in the classified byline. But, we'll let Miss Waller answer that.

Q: The question is whether or not you would have to put the contract number *again* on your classified byline? Isn't that what you're saying?

A: Yes.

A: If I was the IS rep, I wouldn't require that if the contract number already appeared there. Some of the IS reps may do that. It depends on the way you read what's there. It says you will. The contractor *will* put, on the classified byline, the DD Form 254 contract number. If you've got a 254, the contract number should be listed in your classified byline. Would you disagree with that.

No. Let me tell you why we would say that. It seems ridiculous to have the contract number on there twice. I really would say that you don't have

to put the contract number in the classified byline, *if* the classified byline reflects that that is the basis of that particular contract number, which is on the face page — is the basis for classification. The purpose for the classified byline is to show the basis for that classification. It is quite possible you might have a contract, have that contract listed, and then have derivative classifications from something else because it might be a wrapper stocking or something. The point is that the classified byline has got to show the origin of the thing and where you got it from. If you got it from a contractor, it should be listed. Does that make it worse or better?

What we're saying is it would be prudent to put that number on there if that is the basis to classify it by. And if that number is real long, you could just say "refer to the above number in the classified byline." But the point is, it's got to be readily identifiable. You have got to know where it came from. And that is basically all we are looking for.

Q: I'm Fred Daigle of Lockheed in Sunnyvale. The procedural items in the contract are primarily the documents that you originated under the contract. The requirements of any government procedural item is that the contract number, the date, and the originating activity have to appear on the document, and the 254. We should not be quoting many 254's any more because, primarily, all 254's should now refer to classification guides. The new concept is that 254's are really only letters of transmittal of classification guides. We should have been referring to the guidance in the block. But if the 254 is the directive, and it is the one on the contract, we have gotten several decisions that it is not necessary to repeat the number again in the block. I think it is strictly a matter of common sense. It is a single document supporting a contract. It is kind of ridiculous to have to repeat it again in the block. But, we're finding more and more that 254's are not references. All 254's are, as I said, letters of transmittal for classification guides.

Q: Gene Cline, Northrop Corporation. Is it still acceptable to use the "review on" line instead of "declassified on"?

A: Say that again, Gene.

Q: Instead of "declassify" to use the "review on" OADR.

A: I'm not sure I understand what you're saying. You wouldn't use "review on" you would use the OADR.

Q: For our place we had "classified by" and on the 2nd line we had "review on" instead of "declassified on." My question is, can we still use the "review on"?

A: No.

Q: That was unacceptable before.

A: The current marking reqirements have eliminated that "review on."

Q: Tony Correia, Rockwell International. I think that from a policy standpoint, we at Rockwell have said that the contract number (in most cases, it is guides now) but that contract number should be listed where you have steady contracts and there is no guide. You use the number because the "classified by" line and the "declassified on" is one authority. Your contract data requirement lists and procedures is another authority. The Executive Order is the authority for the "classified by" and the "declassified on" statement. All you've got to do is give engineers an out and say, you don't have to use it if you've already got the contract number and you're in trouble. So the best thing that we have found is that it has got to go on there.

Q: Then the contract itself with the CDRL says you have to have the contract number on the documents and reports.

A: Absolutely. Are you talking about the 1423?

Q: Right.

A: The DD Form 1423 is the document, as I understand and remember it from childhood days, which just tells you what documentation must be provided under the contract. It has no authority for classifying. Only your 254 is your authority to classify information.

Q: We're in the middle of several contracts. The

contract is halfway finished and half of our documentation has gone out. Then there is an Executive Order which changes the downgrading requirements. What we've been doing is (until the contract is completed) use the old downgrading used in the first part of the work. Is that correct? To be consistent, I don't think it should be changed. Is that correct?

A: No. I don't feel that is correct. Does anyone want to challenge me on that one? You must follow through with the new Executive Order.

The next set is going to be on the remarking of material orginated prior to 1982 (August 1, 1982). Anything that you are originating now will have to go with the new Executive Order requirements, the new industrial security manual requirements, and you should be receiving revised guidance from your user agency. If you have not, you should pursue going back on your own. Don't wait for them to come to you. I did not press to get those 254's changed because I felt the time and effort should be spent on those things that are required to getting it changed in the contract. I felt that the more important ones to get out were when there had been classification changes on contracts Don't wait for your user agency to come to you. You should go to your user agency. If you do not *receive* the information that you need to proceed on the contract, let us know and we'll do what we can to assist you.

Any other questions?

Q: Gladys Pyatt, Polaris Missile Facility, Charleston, South Carolina. On your "classified by" I noticed you have the instruction and the date that instruction became effective. Is the date required when you use your "classified by"?

A: When you are using it in instruction?

Q: Yes.

A: I'm going to say Yes. I am getting an affirmative from the back of the room. You could have an instruction that had many changes to it. Maybe the original instruction was dated 1976 and in 1983 you had multiple changes since that time. You should identify which one you are currently working under because it is going to cancel and supercede all previous ones.

Q: Then the deed is required?

A: I am going to say yes, it is.

I am going to attempt to answer two questions that have come up during the break.

One of the questions was, on the "classified by" line, do you quote the 254 *and* the classification guide that you have been directed to use by that 254. The answer to that question is *yes*. I have to take it back, Elaine, concerning what I said just a few minutes ago. You will show the DD Form 254, the contract number, and then you will also show the instruction or guide.

The other question that had come up is, on the "classified by" line, what exactly do you show when a single source document is used. In talking with Sandy, you would go back to the contract that that source document was generated under and you would cite that 254.

Q: Shirley Carlston, Baider-Northrup. Suppose you have a document and you are classifying it by the DD 254, but you also have some material that comes from a source document?

A: I'm going to advise that you would say "and multiple sources" and indicate what that source document was.

Q: Are you sure? I think you list the document. According to my advisor ... no? No, you would not. In other words, even though you have one source document, you will put multiple sources.

A: That would be the approach.

Well it comes back again. You only have one document that you are using as your source document. If I am understanding the question correctly, you are not using two documents. You are only using one document to originate another document.

You would cite the DD 254 and the source document that you got the classification from. It is

not a multiple source. The contractor is always the first to use the 254 and any other source. Now that is *not* multiple sources. Does that make sense? The purpose of requiring the contractor to use the 254 as a source document on your "classified by" line is to provide an audit trail in case we need to know why you classified that document.

Q: Jim Mathena, Martin-Marietta. I think what I'm hearing here is that the DD 254 and the contract number must *always* appear on the "classified by" line, regardless of what other sources are used. Is that a correct statement? That's what I just heard. That's exactly what you just said, and that's not the case with the documents that I have seen over the years. Very rarely do I see that situation. There may be a problem here if there is a misunderstanding.

A: I have a feeling we're having a miscommunication and I can't seem to turn it around in my mind as to what it is. Is that a question that we could get back to you on?

Q: This is Jim Mathena again. What I've heard this morning is entirely different than what I talked to you about. The best I remember, and if I had an ISM we could look it up, but I always thought that you could use "either/or." Whatever the appropriate classification or source was, that's what you identify on the "classified by" line. In most cases, I see documents generated by government agencies that come into our facility that do not identify these properly. They always identify the security classification guide because that guide may be applicable to various contracts. They could not be consistent with the way contractors could, because their guides are applicable on various contracts. They cannot identify a contract number on it. So that creates sort of a double standard where a government agency that develops the document must identify the classification guide. Yet a contractor that generates the document must identify a contract number and a security classification guide. I don't think it's written that way. I think it's written that you identify the source of the classification authority.

A: Mary Joe, have you got that paragraph pinpointed at this point? Maybe I should read what it says in the ISM.

Q: This is Junius Layson of Boeing again. I would like to echo what Jim says. I think you will find another situation where you will never find a contract or a classification guide. You may have a classification authority, an original government classification authority.

A: That is correct.

Q: What you're doing is citing the classification authority that is involved, whether that is contained in a DD 254, or security classification guide, or an original government classifying authority. That's the whole purpose, to be able to trace back to what authority you classified the material under. We have many instances. For example, we'll get messages from the Joint Chiefs of Staff. They have classified it. That's our authority. We'll show it's classified by the Joint Chiefs of Staff.

A: We have Joe Grau here from the Defense Industrial Security Institute (DISI) School. He does the classification marking portion for the school, which we all may or may not have gone to. Let's get his approach to this.

Joe Grau *from the Industrial Security* Institute. I don't know anything about ISM requirements. I teach the other side of the house ... the government. My only point is I have a problem with something you just said. Where you get a message from JCS, then you cite on your document — whether you cite a 254 or whatever else — classified by the Joint Chiefs of Staff. I think your proper citation should be to the document that transmitted that guidance, because the JCS has not seen your document and applied an original classification. The JCS has given you direction in some sort of document to apply classification to it. In government, if you derived information or derived your authority for classification from some document, you would not cite the original classifier of that document. You would cite that source of classification which is the document.

Gentlemen, I have pinpointed what the Industrial Security Manual says. Maybe this will help clarify the issue for all of us. It's on page 254 and it's paragraph 2a on that page. Second sentence — because the first sentence is talking about using the 254 as a classifying authority, or other

user agency guide. It goes on to say, "in addition, if any single guidance source other than or supplemental to the applicable 254 is followed, that source will also be shown in such a way that standing alone it will be sufficiently complete to identify it."

Let me give you an example. We get the message in. It has classified information in it. We want to incorporate some of that classified information in a document we have generated. We have no other source than the message and the instructions in the ISM relative to messages coming in that you utilize that source as the classification authority. We have no guidance, no contract, or anything else, except the message that came in which was classified. The originating authority is our source, and that's what we show on our derivative information that's incorporated into the document.

A: If you followed that source, what would you do if you got a document from the government that said "classified by multiple sources"? The government and I don't have to tell you what my multiple sources are. I keep a record with my record copy. You would say then "classified by letter, ODCSR and D,D/A , which is the agency I'm with, dated so-and-so." That's your derivative source for classification.

All I'm saying is that you do not say "classified by JCS." You say "classified by JCS. Message, date, time, etc." You identify the source document itself.

Q: Dean Richardson, T.I. Sheila, maybe we can get off this if I can just make a simple little comment. I'm a user. I have to use these things now. I'm not a supplier anymore, or a derivative classifier, if you want to call it that. Whatever you put on that document, make it complete so that when I want to take that document and sell it to somebody because it is about 25 years old, I've got to know who to go to if it doesn't have a "declassified" line on it. We have got to have declassification times on it. We have got to have a source. I know what Julius is saying. What could he do? It is a bureaucratic "catch 22." He has got to put something down there. But if he wants to get that information to his friends in Germany, he's never going to find who classified it, so he's never going to get it declassified, even if it's 25 years old. All I'm saying folks, whenever you put a mark on a document to classify something, make it identifiable so that we, the users, can find out who it is we have to go to. Even if it is just a contract number, you can usually go back and find an agency to deal with. So we've got to have information — we users — of how we can declassify things.

A: That is basically what I was just reading from, the Industrial Security Manual. Any other question, or shall we go on?

Q: Gloria Ford from COMSAT in Washington. I've found over the years, no matter what source material you have, if you have a DD 254 contract number, you should always apply that. For one reason, when the inspector comes in and he picks up a document, and the DD 254 number is applied, he is going to ask you if this is a current contract. If it's not, you're going to have to ask for a retention authority for that document — even after the contract has expired. It helps you to go back and follow up to see if the contract is still current. I know it's a lot of trouble in putting the contract number and the source material on that little line, but it really helps you in the long run.

A: The whole purpose of using a 254 is to provide the audit trail, among other things. This will provide an audit trail for that document to get it back to the appropriate classifying authority, should there be any questions, because you may have the document for twenty five years. You need to be able to track it back as to what the correct classification is. By having the 254 cited, and the contract number, this will provide that capability for you.

COMMENT: Just to clarify the multiple source question. As I understand it and the instructions I give to our people, we always cite the DD 254, the contract number and the date. If there's a security classification guide only, they'll say that. If the classification guide and some other source document is used, then it's multiple sources. If there's no classification guide and its only source documents, it's the DD 254, the contract number and date and multiple sources.

A: It's always the DD 254 and if there is one guidance besides that, they list it.

Q: You're saying you're going to use the 254 and the other guidance.

A: And the other guidance, if there is more than one, such as using a classification guide and another source document then it's multiple sources.

Sometimes our DD 254's will say your classified by line will read thus and so like an NSA regulation, or something like that. Then, of course, we do it the way the DD 254 says.

COMMENT: This is because you are sending the document back to your customer for issuance by them rather than yourself under their cover sheet.

A: Not neccessarily. No. They just say the "classified by" line shall read as follows on all contracts of new documents. Some say specifically they do not want the DD 254 cited.

Q: If you have a specific directive then from your customer, you will do what your customer says?

A: Right. I am on set four now. The remarking of classified material originated prior to August 1982.

According to all of the referenced documents that I used in preparing this sample set for you, the material originated prior to August 1, 1982. This specifies a date or event for declassification which does not need to be remarked, unless you have received direction from your customer or your higher headquarters. You have received a final 254 or revised 254 and I put it in that manner because when I was issuing the 254's we would sometimes take the avenue of the final to change the classification. Read your 254's carefully. The only other time that you would have to remark the material is if you have taken the document for the purpose of extracting from it, for reproduction purposes, or if you are transmitting that document outside of your agency or facility. The words very carefully in 5200.1R do not mention that material is in the file. Nor do they use the old term of withdrawn from file for use.

There are times when you have information that is unclassified when it is standing alone. However, it would require a classification when it has been combined or associated with other unclassified information. Then the classification is required to protect your total compilation of that information. The overall marking will be assigned to the document. It shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. You will also make a statement at or near the beginning of the document as to why the document has been classified to the level that has been applied.You do not need to further portion mark that document Are there any questions on that?

Now we're going to talk about the marking of working papers.

Your working papers are going to include notes, drafts, drawings or other work that is in progress, that is used to accumulate or create a finished document. When you have a working paper it will be marked with the overall classification and appropriate page markings. It will be dated when it has been created. You do not have to portion mark and you do not have to apply the downgrading declassification instructions, until the material has been entered into the accountability system and made a part of the permanent records or dispatched outside of the facility or activity. My feeling on portion marking of working papers is that it only makes sense when you're in the process of creating that document to take the time to apply the overall marking and it's just as easy to sit down and give it thought as to what that paragraph should be classified and at what level. It is going to eliminate much time and effort, particularly when you are beginning to create a two or three hundred page document. That way you don't have to stop and think, maybe you started it six months ago. You're really going to save yourself a lot of time and effort if you go ahead and do the portion marking. However, we will not come in on inspections and cite you if you have not portion marked your working papers.

Q: I'd like to know on working papers if you have to put additional markings on your document? CNWDI, WNINTEL, etc., that type of marking. Does that have to go anywhere on your draft?

A. Prior to putting into the accountability system?

Q: Yes.

A: I am going to say yes.

Q: I don't think the ISM says that.

A: Well, it would only make sense to do it.

Q: Well it does make sense, except it doesn't say it.

A: Unfortunately, there are a lot of things that aren't said in the ISM. However, I am going to say yes and I am getting affirmative nods from the back of the room. To protect the information, you're trying to tell everyone who has to work with that document that its secret, and if its restricted data they should know that because you can't give that to just anybody. WNINTEL also should be held close and if it's NATO then you've got to have appropriate NATO briefings on file.

A: That's right.

Q: Yes, you do put the other applicable warning notices on a working paper. It's just that you are not required to put the downgrading instructions or do the portion marking, until such time as you enter it into the accountability system.

Q: Kathy Allen, Northrop. I have told our Engineers that are working constantly with working papers, drafts and what-not, that if they keep these working papers for more than thirty days after they are completed, then at that time they have to go into accountability. A lot of these working papers are in a continuous state of updating change. I have told our Engineers that each time they add information to those working papers that they should date it and include it in their drafts. Is it absolutely necessary that they include that date, or is that a requirement that perhaps I shouldn't be imposing on them?

A: If it's material that is being incorporated into a working paper as an ongoing effort, it may take eight to nine months for it to be completed.

The book is saying that you will date it when it has been created. If you are going to further date another internal page it could have a six month's date difference between your first page and ten pages later. I am going to have to ask for council on that.

Q: Are we going to work with more than one date on working papers? For example, if I have started this page August 1, 1982, and I have originated another page on September 1, 1982, am I going to date each page with a different date or am I going to strictly use my first page date?

A: The inspectors have cited us for working papers because those working papers were held longer than they really should have been.They had only an original date on them when those working papers were initially begun. To avoid that, because these things are in a continuous update, I told our Engineers to continuously change that date. Any time they add new information it is the only way we can prove that the working papers are in a continuous state of updating.

A: When you're working on a document and a document goes through multiple stages and its still in a working document format, to me the date that should be on that document is the last date of that draft. As you move that document through stages you should change that date as it goes along because that's the document your working with. Usually, what happens is that document is reproduced. That's when you should put it into accountability. Then if you've read your ISM very carefully, you'll see that's not in the ISM anymore. The reason is that when they printed it they left it out along with leaving out a whole bunch of other words. The new ISM that we've just come out with states that it was inadvertently left out and that is not a change to the ISM so, when you reproduce, it does have to go in. Essentially, you have to update that particular date. If not, then you don't have the time frame to work with. Because the document that you were starting with is effectively destroyed by one compilation into the next document so you'd use the most recent date.

I think we're overlooking the chief factor here, which is,what is done with this working paper.

Working papers are normally something created as a preparatory to the finalization in a neatly printed form. The clock on the thirty day period starts at the time the end item, the final document, is created or work thereon is discontinued. The clock doesn't start with the date the working paper was created. The date that the working paper was revised doesn't matter. The clock is starting when that final document is created. The only reason for keeping up the date is if you stop work on it, that you can track the date. What they tagged you for probably was for not knowing when you stopped work on it and the document was just sitting there for six or eight months or whatever.That's usually what the citation is for. They go in and they look at the document that has been sitting there and effectively no work has been going on.That's the reason they need the date.

Q: Tony Correia, Rockwell International. Having spent 24 years in the bureaucracy of the government you find ways to get around things to meet the regulations. What we did was to generate a project notebook. The project notebook is classified from the very beginning, or from the time that they put classified information in it. All of the project information goes into that notebook. From that notebook, they extract information to comply with quarterly reports, sixty-day reports, or whatever applies. That notebook is classified for the total life of the project. We had some of them that have gone 2½ years. A notebook is classified as new information goes in it every day — test information, status information, etc. We call it a project notebook. It's classified. The inspectors look at it and they extract information to comply with their CDRL items because the whole history of the project is in that notebook and it is classified. I found it's a lot easier than trying to worry about revision dates every time you put new information in it. And that's one way we have found to meet the regulation, and it works very well.

Q: Do you control it?

A: Yes. It's logged and in the accountability system and also paragraph marked.

Q: Dean Richardson, T.I. Sheila, this again is in a user mode. I'm going back to item number 2, under Remarking Classified Material.

I don't see any reason, and I can't see the logic. This is what you have got to tell your people. You've got to make it logical for them. I see absolutely no logic for paragraph number 2. If the document is withdrawn for use — I've got a research document that I have got to extract material from, and I am not going to take the time to go remark that thing if it already has a "classified by" line and has a "declassification" date. If I've got a classified document that I want to send to one of our German friends, and I've got an Export License, I'm not going to go remark that thing because it's got to get over there to be part of an R.F.Q. I don't see any logic behind number 2. I can understand number 1. But, I think if you stop with number 1, it's logical and it makes sense. Remark it if it doesn't have a "declassification" date and doesn't have a "classified by" line.

A: I have only inserted here what I took out of 5200.1R, as well as the Industrial Security Manual. I hear what you are saying, Dean. It's not a case of instructing our people. These are the guidelines they have to work with.

Q: The reason that I bring that up is because we've got the people that write the books sitting right over here on my right.

A: Mr. Williams or Ms. Waller, would you like to respond please.

I guess this isn't going to be a pleasant response on this one. Basically, Dean, we have the requirement under the Executive Order to have the current markings on it. If you took a document out that's required to be remarked in that fashion, I can appreciate the point of view. However, if you took that out and sent that to a foreign government and it didn't have the current markings on it and the exact order, then we would cite you with a deficiency.

Q: How would you know?

A: Well, we would hope that we would be able to detect it during our indepth inspections, and you're so honest, I know that you would tell us, right?

Also we would check transmittal records. We

look for little things like that. Any other questions?

Q: Jim Mathena. I would like to go back to the working paper thing for a minute. I have some thoughts on that. I liked Tony Correia's response on the way he explained how they do it at Rockwell. And, Shirley, if your document is something that somebody develops — this working paper document — and 3 months later they come in and add some new data to it, and Dick says it's permissible to put a revised date on it if the work is in process. That sounds good, but I'm not sure that that's the best thing. Accountability numbers are cheap. And a receipting system — I like Tony's idea, the way he does it. That's the way I've done it. I like to do that. I like to apply a number to it and make the person responsible and accountable for it, because there is really an indefinite period of time that a document can be in a working paper stage. It could be years.

A: I don't think that is necessarily good control of classified information for documents like engineering notebooks and things like that that people are keeping just for source data. If this document is going to reach a final report in a certain amount of time, which most documents do, then, the accountability system will take care of them.

Q: The problem I have with working papers is, what is the definition of discontinuance of work? Is it because I start a document and I go on a 4-week vacation and I quit working on it? Or is it because the contract does not require this document to be completed? I've worked on documents where we've started to develop them for a contract and the user agency said, "No, let's stop that. We really don't want to put the effort into producing this report. Let's discontinue this effort." So at what point-and-time, or what is the definition of discontinuance of work. I think this is something that needs to be readdressed and better clarification placed in the regulation. I'm not sure that any of you have had trouble with that, but it bothers me a little bit.

A: I'd like to agree with Lloyd Kelly's interpretation. We have many documents that are in a working paper status and there is an original creation date shown on it. But if we showed a new date every time it is revised, that would be done on a daily basis. The dates that it is being reworked is immaterial. The sole determiner of when you have to put it in an accountability system is when the individual that is working on it says, "I'm no longer working on it."

I interpret the Industrial Security Manual to say exactly what it does. You show the date that it is created and you are not required to show subsequent revision dates on the thing, as long as it is in a working paper status.

I don't believe I'm going to comment any further on any of that. The various systems, if you're interested in accountability systems, or how other industries handle their working papers and whatnot — I will allow my husband to say *a* word. We have gone in many a time on inspections at Lockheed and, in fact, helped with ESL. I know we suggested they were having a problem with it and we suggested they go to Lockheed and find out how they're handling their working papers. If you would be interested in hearing how Lockheed does it, I will let him say *two* words. But they do have a good system. We have been very impressed with it.

COMMENT: We have probably taken an additional step as to what is really required. We don't allow anyone to start a secret document, working paper document, without getting a preliminary number from Document Management. The preliminary number, and the date you start the document is placed on the working material. You put your warning notices and all of that sort of stuff on that as we've already discussed. If in 30 days you have not completed that document, we maintain a "tickler" in Document Management, and either you have to go back to Document Management and get an authorized extension of that working material date, or indicate you have completed the document and cancelled another. Document Management is authorized to give you three extensions. Each time you get an extension, you change the date on the document so that the inspector knows that the document is under positive control and that within 30 days you have made a decision, and it is still a valid working document. After that period of time, if you still need an additional extension on that document, you have to discuss it with the security rep and justify to him why that document has not been

completed. And it does go on. You do get additional extensions. However, they're practically automatic. The document control clerks, which are hourly personnel, are authorized to give you up to three extensions. We maintain positive control on all working material. It is not formalized and put into the accounting system until you are completed. When that is completed, the document control number then becomes a formal number in our formalized system. There is always positive control.

A: Thank you.We are obviously not going to get through my set, number 5, which is the marking of the portion on overall marking, paragraph marking, and that sort of thing. Hopefully, the sets will be of some use and some value to you when you're back.

*SET #1*

**Classification Pending Marking**

A. *When* & *How* should this marking be used?

1. *Only* when the originator of the material *does not* have an applicable classification guide, DD Form 254, or *has not* extracted classified information from another document, but *does* believe the material should be protected based on previous experience in a similar field of interest which the government has acquired a proprietory interest. In this case the following marking should be applied to the document:

Classification determination pending
Protect as though classified
(Insert CONFIDENTIAL, SECRET or TOP SECRET)

2. The above marking need only to be applied once on the material but placed conspicuously so as to draw attention of the recipient. No other markings are required. However, if desired by the contractor, it is acceptable to add the designation "company private" or "proprietary."

B. Now what step should be taken?

1. Send the document to an appropriate User Agency for a classification determination. Explain why the decision was reached that it perhaps should be classified. "An appropriate User Agency" could be one of the following:

(a) The DoD activity wherein a current contractual relationship exists in a "like" atmosphere.

(b) The Head of a Military Organization.

(c) One of the Agencies listed on pages 252/253 of the Industrial Security Manual.

2. Limit the distribution of this information pending the results of the final classification determination and, of course, safeguard it accordingly.

C. If a response has not been received within 30 days of submission to the appropriate User Agency, assistance may be requested from the contractor's Cognizant Security Office.

*SET #2*

**Additional Markings/Special Access Markings**

In some instances, additional markings need to be assigned to classified documents or other material in addition to the overall classification of the document and appropriate "Classified by" and "Declassify on" markings as shown below:

A. RESTRICTED DATA/FORMERLY RESTRICTED DATA

1. Restricted Data and Formerly Restricted Data markings are evidence of exemption from further downgrading/declassification instruction. However, "Classified by" is to appear on material generated after 1 June 1972, that is based derivatively on RD/FRD information.

2. Remarkings of RD/FRD material originated prior to 1 June 1972, is not required.

3. The following markings would be placed in a conspicuous spot on the outside of the front cover, if any, or on the first page if there is no front cover in addition to the highest overall classification assignment applicable to the document.

Classified by: __

RESTRICTED DATA

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

Classified by: __

FORMERLY
RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act, 1954.

B. WNINTEL

WARNING NOTICE
INTELLIGENCE SOURCES OR
METHODS INVOLVED

1. This marking denotes material which contains classified intelligence information.

2. This marking is to be used when:

   (a) So directed by a classification guide or DD Form 254.

   (b) Extracting information from another document carrying this marking.

3. This marking is to be applied to the front cover, if any, or first page or title page of the document.

C. FOREIGN GOVERNMENT INFORMATION (FGI)

This marking is used on documents which contain foreign government information to ensure that such information is not declassified prematurely or disclosed to a third country without consent of the originating activity.

D. NATO MARKINGS

There are two types of markings which relate to NATO INFORMATION:

1. The following marking is to be used on U.S. documents which contain extracts from NATO marked documents:

THIS DOCUMENT CONTAINS NATO INFORMATION

2. One of the following is to be used on documents to signify that the document is the *property* of NATO:

NATO SECRET
NATO CONFIDENTIAL
NATO RESTRICTED
COSMIC TOP SECRET

3. One of the above markings, as appropriate, would be applied to the outside covers, if any, or first page of the document.

E. CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI) MARKINGS

This marking is applicable when TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA reveals the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device.

1. This marking would be applied when:

(a) So directed by a classification guide of DD Form 254.

(b) Information is extracted from another document carrying this marking.

2. The following represents the manner in which it is to appear on the front cover, if any, or first page or title page of the document:

CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION
DoD DIRECTIVE 5210.2 APPLIES

*SET #3*

**Classifying Authority and Downgrading Declassification Instructions**

A. All information classified by an authorized official within the Department of Defense *must show* the following:

1. Classified by: (See Below)

(a) Use the Date of the DD Form 254, plus Contract No. or IFR, RFQ, RFP No. as appropriate or the designated applicable User Agency Classification Guide.

(b) If "Multiple Sources" are also utilized — add "And Multiple Sources" to 1(a) above. When using this additional statement — records must be maintained to support this phrase and retained for the duration of the contract or program for which the document was created.

2. Declassify on: (See Below)

(a) Show the date/event as designated by the DD Form 254 or User Agency Classification Guide.

(b) Most restricted source document date.

(c) Originating Agency's Determination Required (OADR) if:

(1) The DD Form 254 so designates.

(2) If the DD Form 254 or source material shows an indefinite date or event, declassification review date, or no date or event for declassification.

B. The following is not a required marking and is used only as stated below:

Downgrade to _____on _____(See Below)

1. Use if directed to do so by the DD Form 254 or User Agency Classification Guide or as shown on a source document.

2. Insert SECRET or CONFIDENTIAL and indicate the effective date or event as designated.

C. The following samples of the above are provided:

| | |
|---|---|
| Classified by: | DD Form 254, 28 February 1982, Contract N00123-82-C-1234 |
| Declassify on: | 31 December 1988 |
| Classified by: | OPNAVINST 1234.5, 1 March 1980 |
| Declassify on: | Originating Agency's Determination Required |
| Classified by: | DD Form 254, 3 April 1981, Contract N00030-81-R-5678 and Multiple Sources Downgrade to CONFIDENTIAL on 5 May 1988 |
| Declassify on: | 31 December 1990 |

*SET #4*

**Remarking Classified Material Originated Prior to Aug 1982**

Material originated prior to 1 August 1982 which specifies a date or event for declassification need not be remarked unless:

1. Such direction has been received from the originator, User Agency or by a Revised/Final DD Form 254.

2. If the document is withdrawn for use, such as for the purpose of extracting from it, reproduction purposes, or if the document is transmitted outside the agency or facility.

MARKING OF COMPILATIONS

In some instances, certain information would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, portions of a document classified in this manner need not be portion marked.

MARKING OF WORKING PAPERS

1. Working Papers include such things as NOTES, DRAFTS, DRAWINGS, AND OTHER WORK IN PROCESS or material accumulated or created in preparation of a finished document. This material is to be:

(a) Marked with the overall classification and appropriate page markings.

(b) Dated when created.

2. Working Papers do not require portion marking and downgrading/declassification instructions until such time as the material is entered into the accountability system, made a part of a permanent record or dispatched outside the facility/activity.

*SET #5*

**Classification Marking/Symbols**

A. FRONT COVER, TITLE PAGE, OR FIRST PAGE MARKING —

1. A properly marked Front Cover, Title Page and First Page will show the overall classification at the top and bottom, the document title with the appropriate classification symbol in parenthesis after the title, date of the document, the appropriate classification authority, etc., and the full address of the facility or agency.

B. PAGE MARKING —

1. Interior pages will be marked at the top and bottom of each page with highest classification contained on that page, or designation of UNCLASSIFIED if all portions on the page are UNCLASSIFIED.

(a) As an alternate, overall document classification may be marked at the top and bottom of each interior page when necessary to achieve production efficiency.

(b) Classification of the information must be adequately indentified in accordance with portion marking requirements.

C. COMPONENT MARKING —
In cases wherein there are major components to complex documents, each major component can be marked as a separate document utilizing all other classification marking requirements.

D. PORTION MARKING — (Section, Part, Paragraph or Similar Portion)

1. Mark each portion to eliminate doubt about the level of classification.

2. Mark each portion with its highest classification or mark it UNCLASSIFIED.

3. Mark each portion immediately following its number or letter designation

OR

Before it begins if there is no number or letter designation.

E. PORTION MARKING — FOREIGN GOVERNMENT, NATO INFORMATION, OR CNWDI INFORMATION

1. When foreign government information is included in U.S. documents, that information must be marked to reflect the originating country as well as the level of classification, i.e., CANADA-R, U.K.-S, NATO-S.

2. The above markings would not be applied when the fact that foreign origin must be concealed.

3. Portions of a document containing "Critical Nuclear Weapons Design Information" shall be marked with an (N) following the classification assigned to that portion, i.e., (S-RD) (N).

F. MARKING MATERIAL OTHER THAN PAPER COPIES OF DOCUMENTS

The following procedures for marking various material containing classified information are not all inclusive.

1. Conspicuously stamp, print, write, paint, or affix the classification assignment and other applicable associated markings to the material so that all holders will be aware of the protection required.

G. MARKING CHARTS, MAPS, DRAWINGS, AND TRACINGS

1. Mark the legend, title or scale blocks, in a manner that differentiates between the classification of the document and the legend or title.

2. Mark overall classification on the top and the bottom of the document.

3. When folded or rolled, classification markings must be visible.

4. Applicable associated markings shall be included near the legend or title block.

H. MARKING PHOTOGRAPHS, FILMS, AND RECORDINGS

1. Mark to ensure that the recipient, viewer, or listener will know the classification.

I. MARKING MAGNETIC, ELECTRONIC OR SOUND RECORDINGS

1. A clear statement of the classification at the beginning and the end is required.

2. Containers are to be marked with the appropriate classification and other applicable markings.

J. MARKING FILMS AND VIDEOTAPES

1. Mark the beginning and end of each reel with the classification and applicable associated markings so that these markings are visible when projected.

2. Mark the containers with the appropriate classification and applicable associated markings.

K. MARKING PHOTOGRAPHS

1. Negatives and positives must be marked with the appropriate classification and applicable associated markings.

2. Roll negatives or positives may be so marked at the beginning and end of each strip.

3 Containers for negatives and positives shall be conspicuously marked with the highest level of classification of their contents as well as any other additional (special) marking.

4. All prints and reproductions shall be conspicuously marked with appropriate markings above the face side of the print, if possible. When not possible to do so, they may be stamped or marked on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means.

L. MARKING TRANSPARENCIES, VUGRAPHS, AND SLIDES

1. Classification assignment must be shown in the image area whenever possible. When not possible to do so, mark the border, holder, or frame. Other applicable markings shall be shown on the border, holder, or frame when it is not possible to show them in the image area or in the accompanying documentation or other written notification.

2. When a set of such material is controlled as a single document, only the title slide or transparency requires the other applicable markings. However, if individual slides or transparencies are removed from the set, they must be marked with all appropriate markings.

M. MARKING MICROFORMS (Microfiche, Microfilm, Micro Atrips and Chips, Aperture Cards)

1. The classification assignment and abbreviated applicable associated markings on the medium or container must be readable with the unaided eye.

2. The classification markings within the image area must be readable when displayed.

3. The classification markings must appear at the beginning and end of each roll of microfilm.

4. Decks of aperture cards must be marked with the classification on the first and last cards.

5. Decks of aperture cards must contain a card identifying contents of the deck, the highest classification, and applicable associated markings.

N. MARKING REMOVABLE ADP AND WORK PROCESSING STORAGE MEDIA

1. Removable information storage devices must bear external markings indicating classification and applicable associated markings.

(a) Examples of removable storage devices include:

| | |
|---|---|
| Magnetic Tape Reels | Diskettes |
| Cartridge & Cassettes | Paper Tapes |
| Disk Cartridges | Removable Disks |
| Disk Packs | Magnetic Cards |

2. ADP Systems and word processing systems employing such media shall provide for internally recorded security classification markings to assure that classified information contained therein, which is reproduced or generated, will bear applicable classification and associated markings.

O. MARKINGS DOCUMENTS PRODUCED ON ADP EQUIPMENT.

1. Conspicuously mark or stamp classification on the first page, and front and back covers, if any.

2. Apply other applicable markings on the face of the document.

3. The classification on the interior pages may be applied by the equipment.

4. If individual pages are removed or reproduced, they must be marked as a separate document.

## P. MARKING DECKS OF ADP PUNCHED CARDS

1. When controlled as a single document, only the first and last cards require classification markings.

2. The deck must contain a card identifying contents, highest classification and applicable associated markings.

3. Cards removed and not returned immediately to the deck must bear appropriate classification markings.

(a) A group of cards so removed may be controlled as a separate document and so marked.

## Q. MARKING FILE FOLDERS

1. Files, Folders, Binders, Envelopes, etc., containing classified documents when not in secure storage shall be conspicuously marked according to the highest classification of any classified document included therein.

2. Classified document cover sheets may be used for this purpose.

*DIS WORKSHOP*
*D D 254*

**Jim Lydon**
**Defense Investigative Services**
**Philadelphia Region**

First of all, I would like to say that I sincerely consider this a great honor to be able to conduct this 254 workshop at this national seminar. I certainly want to commend Jerry Acuff and I would like to congratulate John Puckett, and the committee who have worked very hard putting this seminar together. I think it's really one of the greatest seminars that I've been to.

Now, I would like to proceed through this by going over each item of the 254 and make some remarks about each item. After that, we have a two-part practical exercise. We also have answer sheets, and I think you will find that they will be a good resource material for you to take home.

There are 16 items on a 254. That's all. I've been looking at them for a long time. I find that most of the time the items that are left blank or otherwise omitted are 1, 3, 4, 5, 6, 7, 14, 15, and 16. Of the remaining items, which are most of the time filled out, but incorrectly, are 11, 12, and 13. So, let's talk about each one.

In item 1, you are suppose to indicate the highest level of access that will be required for a performance on the contract, regardless of whether the access is to be at a government activity or the contractor's own facility, or at another contractor's facility. It doesn't matter where the access is going to be. The highest level of access that will be encountered is what goes in that block, and there are only three (CONFIDENTIAL, SECRET and TOP SECRET). It doesn't matter whether the access involves custody of material by the contractor or simply access to information only. You should indicate the highest level of access that the contractor's personnel will have. Now, it doesn't have to equal the level of the facility clearance either. If the contractor's clearance is SECRET, you do not have to put SECRET in item 1 if you are issuing him a confidential contract. But it certainly can't exceed what the contractor's level of clearance is. On this, I refer you to paragraph 1-110 in the ISR, or 56-66 in the ISM.

One of the first things that you need to do very early on is to determine that the contractor has a valid clearance of sufficient level.

I know some of you folks are very experienced in this program and probably know more about 254's than I do. But, how many of you are kind of new at this or really don't know much about 254's? Do we have anybody out there? Good. This will be a little bit basic and I was hoping that there would be some folks that would need some basic training in this area of the program. After determining that the contractor does have the proper clearance, then if you are going to release material to that contractor, you must also validate and verify that he has adequate safeguarding capability. Maybe you people call it "squeeze." We calll it "safeguarding capability."

Now you should make these determinations prior to issuing the contract. The 254 is also used with regard to solicitations in the pre-award phase of contracting. Sometimes in the pre-award phase, the bid is not classified at all — many times it's not, and does not require pre-award access. So we ask the user agencies, when they're issuing a 254 for solicitationing and it's not going to require pre-award access, to indicate that. A good spot to put that in would be in item 11.0 at the bottom of the front page, where it says "Remarks." No pre-award access required is a nice way to express that. Because we could issue an unclassified solicitation to an uncleared facility. If in item 1 it says SECRET, and if in item 11 you check custody of material, and you issue it to an uncleared facility then I get upset. You might mention that there is no classified material in the bid package when that's the case. What I'm trying to say is to be specific in the 254. I see many 254's that are terribly vague and it makes you wonder what really is going on.

To verify the clearance, you simply call the Cognizant Security Office for the facility where you are issuing the 254. In user agencies, I refer you to Appendix B of the Industrial Security Regulation which lists the names and addresses, and the telephone numbers of each of the eight COG security offices. The same information is reflected in Appendix VIII of the Industrial Security Manual. A lot of people seem to have the idea that we are still part of the Defense Contract Administration

Services Region (DCASR). We get a lot of 254's and other mail requests for verification of clearances, and so forth, addressed to DCASR, Philadelphia. We have not been part of DCASR since October of 1980. I have a slight suspicion that people don't read Appendix VIII. So, what I did was take Appendix VIII out of the ISM and Appendix B out of the ISR and I'm going to start shooting them back at you. If you don't read it, you're going to get a complimentary copy in the mail. With these incorrect addresses and the incorrect post office box numbers, that mail really gets fowled up. We still see 254's using the COG Security Office, DCASR, New York. Not only are we not part of DCASR, but there is no more New York region. That went out in February 1982. So, take a look at those Appendices when you get a chance and make sure that you know who it is that you are doing business with. I've seen a couple, well several 254's, where in item 16 they indicated us as the Contract Administration Office, DIS. Obviously, the person that did that thinks that there is no more DCASR and that it is now DIS — that we are the Contract Administration Office. That's not so. DCASR is still over there doing business at the same old stand but they administer contracts that we are the Defense Investigative Service — two separate organizations.

Another thing that can present difficulties with the verification processes of clearances and safeguardings is that we experience many cases where the contracting officer calls the COG Security Office to verify the clearance and safeguarding instead of going through the Security Manager of his activity. So you can have a contracting officer in room 22 of an alien activity calling and 2 or 3 other contracting officers calling about the same facilities in the same day, from the same activity, because they are not coordinated or routed through the Security Manager's office. We are trying to encourage them to go through the Security Manager. Some of them are so large that they probably would have some problems trying to do that. But, other user agencies have picked up on that and they are learning to do it that way.

Another thing is that when you call us and ask us to verify the clearance and safeguarding, we reduce that to writing and you would get a copy, and the IS rep in the field office gets a copy. We also file a copy in the central file in the Facilities Division of that verification of that clearance, and it stays in there for a year. So next month you don't have to call and verify that clearance again. If anything goes wrong with the clearance or safeguarding or if anything goes wrong in that facility within a year, we go through that file and we check the contract lists to see what they are performing on. We would notify those user agencies that there is a problem. We also check any requests that came in for clearance verification or safeguarding within the past year and notify the activity that made that request. If you are issuing 2 or 3 contracts to the same contractor within a period of a few months, you only have to make that verification once.

If you are issuing an unclassified solicitation to an uncleared facility, it's advisable to build enough time into your procurred lead time to get that facility cleared, if they should express a bonifide interest in that bid and are clearable. I've seen cases where the procurement time has drawn down to a very narrow gap, and now the user agency wants the facility cleared in 2 weeks, and it takes like 4 months or longer, if it's TOP SECRET It is well to consider how long it takes to get the facility cleared when you are planning your procurement lead time. Keep in mind that the 254 that you send to the Cognizant Security Office, if and when you do (alot of you don't), is not a request to have the facility cleared. If you are dealing with a facility that is not yet cleared and you want us to clear that facility, then you must write a letter to the Facility Division of the appropriate Cognizant Security Office and request that the clearance process be initiated, and your letter must include adequate justification. Sometimes, in the justification category, the user agency will attach a copy of the 254 and still express some narrative justification in their request letter. It costs alot of money to go through the procedure of clearing a facility and we get some outrageous requests for access only type situations. There are some government activities who think that where you have a "controlled area", some of them call them "classified areas", that the first thing you have to do is clear everybody who visits there. That's not the first responsibility at all. The first responsibility that a user or activity has is to establish security controls that will effectively deny access to the personnel that have to come into those areas. If you can do that, then you don't

have to have the facility cleared. Some people will say, "well that costs money". What difference does it make whether it comes out of your budget or ours? You know, it still all comes out of the same taxpayers' expense.

I had a request recently, and this guy was serious. I thought it was a joke. I thought somebody in the office was pulling a funny one on me. He called up and wanted us to clear the Philadelphia Gas Works. I asked him why. He says, "Oh, they have to come in here and read the gas meter." I said, "Well I know. When the guy comes in to read the gas meter, keep an eye on him. Follow him around." He says, "Well, what if they had a gas leak and they had to send a crew in to repair it?" I said, "When did you have the last gas leak down there?" And he said, "Well, we never had one." I said, "And you want us to clear Philadelphia Gas Works just in case you do." This guy was serious. I couldn't believe it. Because the victim's idea is that if there is the possibility of inadvertant access, you have to get the people cleared. You don't. Your first responsibility is to establish security controls that will effectively deny access. If that costs a little bit of money to provide an escort, keep an eye on these people, or cover the classified material, that's what you are suppose to do. Let's go to item 2.

The 254 can be used in three different ways. Item 2a would indicate that it is being issued for a prime contract by the user agency. Item 2b would indicate that it is being issued by a prime contractor for a subcontract to another contractor's facility. It could be the first tier issuing to a 2nd tier. Or, it can be issued to a solicitation. Whether the solicitation is classified or not, the regulation does say that if the contract is going to involve access to classified information or material, then the 254 must be issued with the solicitation. The contractor knows then when he's preparing the response to that request for a proposal that it is going to be a classified contract. The best way to inform him of that is to put a 254 in the solicitation package.

You will notice that item 3 calls for an identification of the procurement action. We normally refer to that as the contract number. Usually, that consists of a 13 digit number. The first 6 digits, which are alphanumeric, identify the contracting activity, such as N00024 (NAVSEA) and 00019 I think would be NAVAIR or NAVELEX, etc. The next two digits identify that fiscal year in which the funds for the contract are budgeted and committed. There is an alphacharacter (usually a "c", but sometimes you'll see an "a" or a "q") which indicates what kind of a procurement action it is — a request for bid, a basic order agreement, an open end contract, or just a regular ordinary negotiated contract. The last 4 digits are actually the contract number. Alot of times, the item 4 date to be completed, estimated date to be completed, or in 4c, the due date of the solicitation is left blank. We like to see that filled in because when we go in to inspect the facility later on and we see that that date has expired, the obvious question is "What did you do with the classified material? Is the contract actually completed or not?" If that date has to be extended, then it is not necessary for you to issue a revised 254. You can extend the date by issuing a modification (MOD) or contracting formality you have to go through, but you don't have to revise the 254 to extend that date. It is a good management tool for us so that we can inspect the facility to find out if the contractor complied with the requirements of returning the solicitation material or if he has requested retention authorization or transfer of accountability, or whatever.

You have item 5 which asks for the current date on the original 254, the date on the revised 254 and a final 254. On original 254s I refer the user agencies to paragraph 7-102a 1 & 2 of the ISR, which explains when an original 254 is required. The revised 254 should show the number of the revision (like revision #1 or revision #2), the date of that revision, and carry *forward* the date of the original 254. You should do the same when you issue a final 254. When you issue a revised 254, indicate what revision it is — 1st, 2nd, 3rd, or whatever and the date of the revision in item 5b. Also carry forward into item 5a, the original date.

Q: Why do you also use the original date?

A: Well, it would help us to see how far back the classification on the contract goes.

Q: Also, a reason to use the original 254 date is that sometimes guidance is provided on the

original 254 that you have to apply to the revisions.

A: It is helpful to do that. I may not be able to explain to you, convincingly, why — but it is helpful. And it's really no problem to do that.

There are only two circumstances under which you would issue a final 254. The first is when upon completion of the contract all of the classified material that was used or generated in the performance of that contract is declassified. Then you issue a final 254 to communicate that information to the contractor. The second one is that when the contract is completed and you want to authorize the contractor, to retain the classified material. You will specify a specific length of time. That's different from transfer of accountability to another contract. We'll talk about that in item 6.

Q: When you issue an original 254 do you also have to issue a list of classified documents to keep them retained?

A: Well, the contractor should have done that when he requested the retention authorization, in compliance with 5L, of the ISM. If there isn't any request for retention, then paragraph 5m of the Industrial Security Manual tells the contractor that that material is to be destroyed. That's exactly what he must do to comply with the requirements of the ISM. If you don't want the material destroyed, then you have to tell him what you do want. Either you want it returned or you want him to use it on another contract, or you want him to retain it for 3 years, whatever. But the ISM tells him to destroy it, period.

Transfer of accountability, loosely speaking, applies to permitting the contractor, when he has completed the one contract, to continue having custody of the classified material residual to that contract for performance on a current, ongoing contract. You can do that very neatly in item 6 when you issue the new contract — a follow on contract, by simply saying that the material is transferred to the follow on contract. That's all you have to do. If it's not a follow on contract, then you can authorize him to transfer accountability of the material to another ongoing contract by way of letter. You can write him a letter. However, in the letter you should indicate that you've reviewed the classification requirements and no changes are required.

Q: When you request retention, to whom do you write, the contracting officer of the contractor to which you want it transferred, or to the original one?

A: To request retention authorization, I would think that you would write to the contracting officer.

Q: I mean, how does that get communicated to the contracting officer on another contract in the same field of interest.

A: You are talking about transfer of accountability from one department to another department. Is that what you are saying? Or one activity to another. Let's say you have an NAVELEX contract. And you also have a NAVAIR contract. You complete the NAVELEX contract but you could use that material on your NAVAIR contract. Now what you have to do here is get NAVELEX to say "we do not object to the transfer of accountability of this material to the NAVAIR contract." They route that through NAVAIR and NAVAIR says it's OK with them too. There should be some coordination there.

Q: Well I still don't know who to write to.

A: To the gaining activity.

You could also ask the original contracting activity for straight retention. With retention authorization, the Industrial Security Regulation requires the Administrative Contracting Officer (ACO) to indicate a specific length of time (1 year, 2 years, 3 years), whatever. Whereas, with transfer of accountability to another contract, the length of time would be for the performance life of that contract. Then when that contract is completed, paragraph 5m of the DOD ISM applies — destroy the material or request retention.

Q: As a contract closes and you have another contractor in which you can use these documents you write to the contracting officer of the open contract and you don't have to do anything with the old contract ...

A: Well, yes.

Q: On the follow on contract ... what happens if your contract isn't completed yet and you have the follow on contract and it is 2 or 3 months before it will be completed ...

A: Well, you could put the date to be completed. I don't see anything wrong with doing that.

It's advisable to reflect in item 7a the name and addresses of the contractor in the manner in which we have in our records as a cleared facility. Now you have some problems with multiple facility organizations. Some locations, which are not clear, and also with off-sites. Now, raise your hands, those who don't know what an off-site is. Sometimes a cleared facility will have another building a mile or two down the road which we have approved as an off-site under certain rigid circumstances. It is improper to issue the classified contract to the off-site, unless there has been a waiver approved. You don't reflect the off-site name and address in the 254. You work with the cleared facility. If it is a multiple facility organization, and you are issuing a service type contract to them, where they are going to furnish cleared personnel to your facility to perform some kind of a service for you, and the cleared personnel are coming out of an uncleared multiple facility location — which they can do, you don't issue the 254 to the uncleared location. You issue it to the cleared home office or principle management office. If you need help in finding out who that is, ask your local cognizant security office for advice on that.

The federal supply code number in item 7b is no longer an absolute requirement like it was when we had that computerized contract list situation. It does help us to specifically identify the facility that you're dealing with when there are, let's say, several locations of the facility, like IBM or Westinghouse, or General Electric. If you put the federal supply code in there, it will be furnished to you when you call and ask for the verification of the clearance. We routinely tell you the level of clearance, safeguarding capability and the federal supply code number. So use that in there. Please make sure that you get the name and address of the cognizant security office correct.

Q: Jim, would it be better to put the classified mailing address that we get if it differs from a physical address. Does it matter to put it in block 7a or to put it under remarks or something?

A: You could put the location in 7a and right under it in parenthesis, if you want to, you could put the classified mail post office box number.

Let me show you that there is a tricky little asterisk after item 7a, and it refers you to that line right above item 10, which says that when actual performance is at a location other than that specified in 7a, then identify that location in item 15. You may be issuing a contract to an IBM facility in New York City, but the actual performance will be done by an IBM facility in Camden, New Jersey. It's the responsibility of that cleared facility to furnish a copy of that 254 to the performing facility and the performing facility's cognizant security office.

Item 8 is used for subcontractors. The prime contractor indicates himself in item 7 and indicates his subcontractor in item 8. If you're issuing the 254 for solicitation and you put the contractor's name and address on it, it should go in item 9. If you're sending that solicitation out to several facilities — what you can do is issue the 254 *blank* in the contractor's name and address block under a letter of transmittal saying "attached solicitation for (and give the solicitation number) has been forwarded to the following facilities in your region." Then you send that to the appropriate cognizant security office. I've seen them come in with as many as 25 or 35 names and addresses of facilities on there. That's perfectly acceptable, providing that when you issue the contract you issue a new 254 — an original 254, with the contract number on it and the contractor's name and address. You don't use the same blank 254, which I've seen a lot of user agencies do.

Q: In the case of a multiple facility, for example, we have an office in Washington which is really the marketing office. They don't have any contract separately. Does that mean that I have to issue a DD 254 to that office?

A: Is this a liaison office?

Q: Yes. More or less.

A: No.

Q: But they are a separate facility and they have their own facility clearance. When they inspected them they may have a copy of our contract DD 254.

A: That's right.

Q: This is their home office. They could use that, but they are not performing exclusively on that contract.

A: With that type of an operation, as long as they're not generating classified material ...

Q: Yes, right. So I don't have to give them the 254?

A: No.

Q: In our user agency we are charged with reviewing for accuracy the 254's. The biggest headache we have here is that sometimes the contract officer issuing the RFQ's will send us 50 names of facilities for verification of clearance. We have to go through 50 names and ensure the verification of a cleared facility before we issue an RFQ.

A: It's like I said earlier ... if you're sending that solicitation to any uncleared facilities, which you have a perfect right to do, if the solicitation does not require pre-award access and there is the possibility that you might want to issue that contract to a facility that isn't cleared, it's a good thing to know about that as early in that procurement action as you possibly can. Because if you wait until it's time to issue the contract and you've got a production schedule and delivery schedules that are involved in that, you're in big trouble. So it's highly advisable to establish that fact as early in the procurement action as you can. It depends on how broad you want your supply base to be. If you are dealing with some sole source type of situation you don't have that problem.

Q: You're not saying that if you get 50 companies that could bid and 5 of those companies are uncleared, that you should establish facility clearances with these other companies?

A: No. I'm not saying that. But what I am saying is if one or more of those 5 companies indicates a bonifide interest in bidding on that package, knowing that it's going to be classified and that they will have to go through the traumatic experience of being cleared, then that could very well constitute justification for our initiating the clearance process. That fact would mean that they are an interested and a capable bidder.

In item 10, it says "general identification of the procurement" and it's awfully clumsy language. Really all that we're asking for there is to give us a description of what the contractor will do (manufacture something, perform some kind of research and write a report, graphic art services, or whatever), just a brief description of what the contractor will do.

In item 10b, it asks for "a DODAD number." That's a user agency number. We really don't need it any more, so if you don't know what your Department of Defense Activity Address Directory (DODAD) code is, don't worry about it.

In item 10c it asks if there are any security requirements additional to those ordinarily required by the ISM. It's expressed a little differently here — it tunes in on the ISR. But really, what they're asking here is "are there any special program requirements?" Now let me give you an example. If you have secret material in your custody that you are using in the performance of a contract, the Industrial Security Manual does not require you to maintain an access register each time someone with the need to know has access to that material. If the user agency that you're dealing with, feels that their material in this case is extra sensitive, they have the approval to initiate a special program and they may ask you to do that. They may require you to have an access register for that secret material. If that's the case, then they should indicate "yes" in item 10c. That is an additional requirement. And they should identify, as well as they can, what the special program is (like Operation Shoelace, or whatever), because we like to find out whether that is an approved special access permit. I think there are a few out there that aren't. The next item refers to a carve-out. It says "are there any elements of this contract which are outside the

inspection responsibility of the cognizant security office." If that's the case, it is a carve-out and usually it involves Sensitive Compartmented Information. So item 10c is related to item 11k — special access. Item 10d is related to item 11j — SCI. Normally you see those together.

Let's talk about item 11 a little bit. You'll notice that the first item in item 11 says access to classified information only. Now I would like to emphasize two words in there and those two words are only at. Only at a government activity or another contractors facility. What that means is that the contractor receiving this 254 will not have access at his own facility. Therefore, no classified material is being sent to that contractor and he does not require safeguarding. If you are sending classified material for him to use as reference and not generate additional classified material, then you would indicate item 11b. But, if generation is involved from a classification guide or derivative classification from source material, which you provide for the contractor, then you would indicate item 11c. You would also furnish him with marking instructions. Now the industrial security manual does not furnish the contractor with marking instructions. It furnishes the contractor only with remarking instructions. It tells the contractor how to properly remark classified material, but if you want that contractor to generate classified material then you need to tell him how it is to be marked. Now, obviously, those three items are contradictory. So, there should be only one checked yes. It's amazing how many times I see all three checked yes. And all differ.

Q: Do you think that where you have the contract involving both SCI and collateral and given a scenario where collateral is held at a contract facility and SCI is only at a government facility you could elaborate in block 15? Is there an easy way to do it as far as throwing out block 11?

A: I would indicate SCI in item 11 and then explain in item 15 that access to sensitive compartmented information will be restricted to government activities.

Q: Is there any problem on 11a identifying SCI only and in 11c identifying SCI only or collateral? In other words what is the more preferable way to do it?

A: The way I just said. By explaining in item 15 that the access to SCI is restricted to government activities. But if you also have collateral material at the facility. Does everybody know what collateral material is? Some material called sensitive compartmented information material comes under item 11j and most of the time it eminates from NSA (National Security Agency). In the contractor's facility, if he is in custody of SCI material, he normally needs to go to a special closed area which NSA would inspect and approve called a Sensitive Compartmented Information Facility (SCIF) within the facility. When we go in and inspect we're not allowed in there because that's a carve-out area. But, in the facility for that same contract he may also have other material that is not in that SCIF, because its National Security Information, not SCI. Does everybody understand that? Now we would have inspection responsibility for that material. So, you see you have to be pretty specific when you are issuing the 254. If there is classified hardware involved you have all kinds of problems. And again, the challenge of being specific is very much involved. Let me give you an example. This ring is a piece of hardware. It could very well be classified. You could take hundreds of these rings and store them accurately in a regular GSA security cabinet and not require a closed area at all. But this podium here, let's say this was a piece of hardware, and its classified. You're not going to put this in a security cabinet, so the contractor in that case would need a controlled area. More than likely he would need a closed area. The difference is that in a restricted area the area restrictions are in effect during working hours, and after working hours the classified material is put away. In a closed area the material is of such a nature that it has to stay in the area. Therefore, the security restrictions of that area have to safe-guard the material. When you indicate hardware, you kind of tell us something. Another thing about hardware is that some hardware items might be classified because the external view of it is classified. Or, it might not get classified until a certain component part is installed. For instance, my wristwatch could be a classified piece of hardware. But, it doesn't become classified until those numeral are put on the dial. That's when it becomes classified, when that dial is installed. That could be the last step in the production process and all the way up to that point, its unclassified. So, you have to tell the

contractor what is classified about the hardware, when it becomes classified, whether or not you need to know, and whether he needs an area to keep it in. We need to know that too.

There is a whole section in the Industrial Security Manual which outlines what the security requirements are for graphic arts. Section roman numeral 10. No problem, you don't have to indicate generation, custody, reference material or anything else. All you have to indicate on graphic arts is item 11b. You would also indicate if restricted data or similar data is used.

Access to IPO information. Does everybody know what IPO means? I didn't know what it was either when I first saw it on this new 254 form. I learned two things, trying to find out what IPO meant on the 254, and I also found out that the new ISM contained a glossary, which it never contained before. It tells you in there that that means International Pact Organization information such as: NATO. If the guy is gonna have access only at 11a, but in that access he's gonna have access to NATO, then you need to indicate that too. There will be some briefing requirements that need to be complied with. Or, if Restricted Data is involved, that should be indicated. Why? Because a contractor issued clearance is not sufficient for Restricted Data. There has to be a final U.S. Government clearance. So, if your sending something out to a print shop on a graphic arts subcontract and it contains Restricted Data, you have to indicate that. This is because the graphic arts guy can't assign a company cleared technician to print that job. It has to be a government clearance. The COMSEC and CRYPTO supplement is being revised. You heard about that yesterday. I think they said its gonna be on the newstand in around ninety days or something like that. About all I am prepared to say about that is if COMSEC is involved, a COMSEC account will be required if the contractor is going to have custody of COMSEC accountable material. All classified material is accountable to a certain extent, but COMSEC accountable is something else. That's an additional requirement. Indicate that COMSEC account is required or COMSEC account is not required, because not all COMSEC material requires a COMSEC account. CRYPTO is required and they are going to have access to on line traffic, as opposed to testing information, indicate that, because then we have to have an account. We have to have a special reason for the facility security officer and he has to establish and appoint a custodian, and an alternate custodian. So, those items are very important in that type of situation. We talked about the SC1 11j and the 11k special access programs. Last year, our friend Irv Boker and his outfit GAO (General Accounting Office), did quite a study on the volume of special access progams and carve-outs and there seems to be a sense of alarm about how much of that there is and how much of it probably is not approved. If access to U.S. classified information outside the United States is involved, in otherwords if you had a contract and it requires that you send cleared employees overseas for longer than ninety days TDY, then you should tell your faithful Cognizant Security Office where they are and what contract they're performing on. But if they're in Heidleburg, tell us they're in Heidleburg. How many current employees do you have there? We need to know because we now send a copy of the 254 to our Office of Industrial Security International in Belgium.

Q: We have an unclassified program on the F16 program. We have 5 people stationed overseas at U.S. Air Force bases and security requires that they have a clearance. Why don't we have a 254 on that contract saying that it requires secret access?

A: Well, it sounds to me like there's something wrong there. If you are required to furnish cleared employees to perform on that contract overseas, that is not an unclassified contract. It should read that it is a classified contract and you should have a 254. I recommend that you talk to your contracting officer about that and, if necessary, your classification management specialist at your cognizant security office. That sounds like a classified contract to me.

The contract instrument itself is never classified. How many times do you see a contract document that's classified? I am sure there are some, but it is rare.

Classified, in my opinion, is the requirement to furnish cleared personnel. If that is a valid requirement, that's a classified contract, because

it implies that employees are having access or will be required to have access.

Q: The naval shipyard requires just to go into a certain area that you have a clearance.

A: When we were talking about item 11a; there are times when that requirement is an overreaction. We try to save that as much as possible. You get some of these guys who wear a captain's hat or an admiral's hat and they want everybody to be cleared, the paper boy, the gas company and everybody.

Q: I agree, but what I am saying is the requirement may be because you're going to have a look at a totally separate piece of hardware or something that has nothing to do with your contract, but your going aboard a ship where there is other classified material in the area.

A: It's for access. If access or inadvertent access is involved or can not be denied, then you have a classified contract.

COMMENT: I would like to add a few things to that. At the NSA we have a few of those contracts and we do have contractors who are unclassified and uncleared. They come in and they may maintain our equipment for us. The equipment that they are maintaining may not be called classified, in some instance, but the fact that they have come into our agency and have potential for access, they have to have a DD 254 written for that purpose. Now the 254 is written so that they could possibly have access in the building. This enables us to process them for a clearance. That is how we cover access into our building.

A: There are times when that can be done, and there are other situations, such as NSA, where it can't be done. But this is for the activity to evaluate what the situation is. It used to be that anybody that went into one of the classified installations near the capitol required a clearance. You couldn't even get inside the gate without a clearance to cut the grass or to wash the windows. They have changed that considerably. They have reduced the number of clearance requirements a great deal, because they began to realize that it is a terribly expensive way to handle security controls. Don't forget that more than a clearance is required to justify access to classified information. What else is required? The need to know. Sure. So you are not really solving the problem by clearing everybody.

Q: I think you will find in some cases it is a matter of convenience on the part of the user agency. If you go back to them and say "I do not have a DD 254 card that covers me for this type of visit on an unescorted basis." They will probably make arrangements to escort you and preclude you from getting into an access area.

Now there are two other items on Item 11. One has to do with the Defense Technical Information Center (DTIC). With regard to that item, I refer you to appendix I, roman numerial I, paragraph T as in taxes in the ISM. It explains what the procedure is for a user agency to sponsor a contractor to receive material from that Documentation Center. There are a couple of forms that have to be filled out and validated by the cognizant security office. It is pretty well covered in that appendix. Item IIn is very much like item IIc. You recall that item IIc means that the contractor will have classified material in his own facility and will generate classified material in his own facility. And that is exactly what item IIn implies. That the contractor will process classified information in an automatic data processing system in his own facility. His own ADP System. Section roman numerial 13 of the ISM outlines in enormous detail what the contractor is required to establish in the way of system safeguards. He has to write a supplement to his SPP and it also has to be approved by his local cognizant security office. Now, if the contractor is coming into your user agency to work on your computer, but to help you to develop some software or program, that is not IIn. That is IIa. If he is working on your computer that is IIa, but if he has his own at his own facility that is IIn and that triggers a great deal of interest on our part as to whether or not he has an approved system.

A: EDP does not necessarily mean a great big computer. It could be a desk top computer, it could be a word processor or a computerized, automated graphic arts type of machine. There are a lot of things that section 13 covers.

Q: If you have a typing service do you check

11e, because they're going to type on a word processor? Do I also have to check yes on IIn if a classified report is involved?

A: If you are going to employ a typing service and you are going to require them to be cleared. It would be primarily their responsibility to make sure that they have cognizant office approval for the equipment that they will use to process classified information.

Q: I don't know if anyone is interested, however, if you could quickly go over these and say which are the cost factors to your company. In other words, if you have to have a closed area and you do not have one currently, that is going to cost you dollars. If you have ADP, you are going to have a cost factor involved. It is important to make the managers aware of the cost factor so you can bring this up to your management or contracts people in the negotiation, particularly in an RFQ. But, you point them out, because they may not be aware of them.

A: Sure. If an RFQ comes into your facility and it indicates classified hardware, it is extremely important for you in evaluating cost factors to determine whether or not you do have to construct a closed area in order to perform on that contract. If ADP is involved there is tremendous cost factor.

I didn't mean to skip item 12, that is terribly important because whoever signs is certifying to the adequacy of the classification guidance that is being furnished. That person also has the responsibility of furnishing to the contractor copies of classification guides that are incorporated by reference in the 254 and also furnishing the contractor with revisions to that guidance as necessary during the performance phase of that contract. I have had the alarming experience on numerous occasions of calling the one who signed item 12 to ask a question concerning the 254 and I got — Huh? I find that alarming. In one case it was a Navy captain. I said, what do you mean Huh? I said, why did you sign this. He said, oh, I sign alot of forms. I said, oh yea. Did you ever have a security violation in your career file, pal? How would you like that to happen to you? He could not answer my question about some security matter on that contract. A Navy captain. I find that alarming. So when you sign that make sure you know what you are doing.

Item 13. We have an editorial boo-boo in the fine print on the second line where it makes reference to appendix roman numeral 9. Roman numerial 9 no longer refers to public release. The information that was contained in roman numerial 9 concerning public release was added to paragraph 5o when the ISM was revised, but we overlooked revising this reference so make sure you don't get confused on that point. Keep this in mind, I think it was mentioned here yesterday, that the restrictions concerning public release apply not only to classified information about a classified contract, but *all* information about a classified contract. So before you release information concerning a classified contract that you are performing on check with your contracting officer, or the guy in item 12, or the public information office of the user agency to make sure that the information that you want to disclose is in fact releasable. Do this before you go to the seminar and give your speech, because that has happened.

In item 14, which is one that is almost always overlooked, there are some interesting things. First of all, it tells you that you have to tell the contractor what elements of the contract are classified. There is a number of ways you can do that. You can write a narrative or you can furnish him with a classification guide, which is the most efficient way. Most of the user agencies are using that to communicate that detailed information to the contractor about every element of the contract that is classified. It must tell him the level of classification, the duration of the classification, and the date or the event of declassification. We see a lot of OADR's rather then declassify on such and such a date. You are allowed to do that, you know, you don't have to say OADR. If you are including a completed narrative, check item 14a. If you are transmitting that under separate cover, indicate that in item 14a2. If you are listing classification guides or a classification guide as being incorporated in this 254 by reference, indicate that in 14b. If it is a service type contract, such as graphic arts, guard services, equipment maintenance or something of that kind, indicate that in 14c. If this is a final 254 authorizing the retention of classified material from a completed contract,

then indicate that in item 14d and also indicate the extent of the retention authorization. The expiration date is a requirement. Another editorial boo-boo is where it says, in 14e, annual review. It should say bi-annual. Every two years. That applies to contracts involving generation of classified material. If generation is not involved then I see no reason why it has to be reviewed.

In the distribution, user agencies, please don't forget the cognizant security office of your contractor. Make sure that we get a copy of the 254. There is no substitute for user agencies, and there is no substitute for the cognizant security office. We have had the experience where a user agency, because they felt that it was a carve-out and very sensitive, thought they were the cognizant security office. They didn't send us a copy of the 254. They didn't just carve us out; they cut us out. Just recently we had a case were we went into a facility because it appeared to us that they had no top secret access in a long time, and they were in fact performing on a top secret carve-out sub-contract which the user agency had cut us out of indicating themselves as the cognizant security office — which is wrong. We had to go from headquarters to headquarters on that one. There are eight cognizant security offices and they are all under DIS. We maintain the facility clearances, and if it is a carve-out we will respect that. As long as it is a valid, approved carve-out we are not going to come intruding and demanding access when we are not suppose to have it.

With regard to signing the 254, obviously if you are a user agency it should be signed by the PCO, the ACO, or a contracting officer representative for security matters or some official of the user agency should sign off in item 16. If you are a prime contractor issuing the 254 to a sub and it involves the transmission of classified materials to the sub-contractor for his use in performance of that contract, as opposed to graphic arts, then it should have an ACO, PCO signature. If you are releasing the user agencies material to the sub-contractor for his use in performance on the contract, the ACO is to know about it, and indicate by signing the 254. If you are issuing a sub-contract for a service that does not require the transmission of classified material to the sub-contractor, other then graphic arts, then you are authorized to sign the 254. The facility security officer usually will do that. You don't have to sign in item 12 and item 16. In that case, when you get to item 12 you can put "see item 16." Remember to put your phone number in those signature blocks. Put the address of your activity or facility and your telephone number and if you are a government activity, the autovan number. If there is any question or problem, we can call you without spending three or four days trying to find out what your phone number is. It is a big government, and trying to find some guy's phone number can be a real job. So put that in there.

Now, you know what? We were going to have a training exercise. I blew it, I talked too much and there were a lot of questions. I do hope that between what I said and what you all asked that it was of some help to you. Maybe you did get some clarification. I want you to take the training exercise and here is what I'm going to do. I have a whole bunch of hand out material here, and two of the items are the answer sheets to the exercise I put on each table. I put eight copies on each table. So that you will find the answer sheets, it will be marked task 1 and task 2. They will be the completed 254's to show you what your 254's should look like. You have to promise me that you won't look at the answer sheets before you do the exercise. (See tasks at end of talk)

Q: Of the current problems I have found with some of the DD 254's, the product managers, the program managers, and some of the user agencies are issuing verbal modification to that and there is no DD 254 sent to reflect this change. Also, on the classification guidance, you may receive a prime contract for only a portion of the overall contract and they are sending you 1500 pages.

A: Let me address both of them. If there is a change in the security requirements on a contract it is improper for the program manager to merely make a phone call to the facility and handle that by telephone. There should be a revised 254. If you are changing the level of classification from SECRET to CONFIDENTIAL, or if you are extending the classification to other items that were not previously classified, then you should issue a 254. I think you have a contractural responsibility. That is a contract specification, that 254. In some user

agencies I notice that they scupulously issue a contract modification as well.

The other item the gentlemen mentioned was about the classification guide. Let's suppose that you are a Navy activity and you have a program for a classified aircraft carrier. You could imagine what the security classification guide would look like. But, you are engaging a prime contractor to build a depth gage that's classified. You don't issue him the classification guide for the whole damn aircraft carrier just to build a depth gage which maybe could be handled in 10 or 15 pages as opposed to 25,000 pages. I know I'm exaggerating here, but that has happen and the contractor is out there and he has this voluminous classification guide and all he is making is a ball point pen or something. You can imagine how hopelessly confused he would be. So you extract from the classification guide, the guidance he would need to perform on what you are contracting him to do. The same thing with a sub-contract. You may be a large aircraft manufacturer and you might have, let's say the F-14 or the F- 16, and you can imagine how big that classification guide would be. You are going to contract out to some guy, and all he is going to make is the nose wheel or windshield or something, but it is going to be classified. You don't have to send him the whole classification guide for the whole airplane, just send him what he needs. Again, you need to know the principle involved. If all the guy is going to make is some little gauge in the instrument panel that's classified CONFIDENTIAL he has no need to know what else is classified in that aircraft. You not only confuse the contractor, but you violate the need to know principle as well.

Q: One more Jim, I think it should be pointed out to the people that some of the contractors are under the impression that access to SCI material which involves the SCIF and a carve-out program are one and the same. They are two different programs. The user agency can deny DIS cognizance to a carve-out because they want to maintain that and DIS does not have access to that sensitive material. They just want to maintain the cognizance themselves. It does not have to be in the SCIF.

A: What he is saying is not every carve-out involves sensitive, compartmented information enclosed within the controlled area of a SCIF within the facility. We have had the experience where we come into a facility and we are looking through the material, and let's say in a four drawer GSA security cabinet, and the security officer says, "I cannot allow you to see the material in that bottom drawer." And the IS rep says "Why not?" and he says "It's a carve-out." Now we have asked the IS rep to open the ISM to the paragraph that lists the names of all the user agencies. Just ask the security officer to look at them and tell me is it one of them? If he says yes, then you know it is a user agency carve-out. But, if he says no, then you know it is non-user agency activity in the facility, and we simply make a note of that and notify our headquarters, DIS, and ask them to attempt to verify for us that it is a valid carve-out and we do not have security responsibility. Not all carve-outs are SCI. All SCI's are carve-outs, but not all carve-outs are SCI.

Q: Maybe this is not the appropriate place for it, but can you challenge a 254 classification?

A: Positively. You should if you feel that there is evidence or indication that perhaps over-classification is involved. Sometimes, the way you might become aware of that is you might have a contract from an Air Force activity fo an item that they classify at the level of confidential and then you get a contract from a Navy activity for the exact same thing and they have classified as SECRET.

Q: For example, in the electronics business it appears that a lot of the classifications are based on old technology, and the classification takes into consideration tubes which are very narrow-banded and the new solid state of technology is very broad-banded. It appears that people are putting classifications on things which, for instance, we sell to commercial accounts and can be bought by any commercial account. I have heard we can't make anything you can buy in Radio Shack.

A: You can challenge the classification on that and should. Now, of course, the contractors are in a ticklish situation because the user agency is your customer and you operate on a profit and loss basis. You would be reluctant to offend your customer and lose a contract or future business. It shouldn't be that way because it all comes out

of the taxpayers pocket. If you do get caught between a rock and a hard place in that kind of thing that's what I'm getting paid to get involved in. If you have a contract out there and you think it is over classified, because your selling the same damn thing to Woolworths 5 & Dime, and you can't get any satisfaction from the contracting officer then you should approach your cognizant security office on it.

Q: Alright just for the record this does happen and we have seen situations where most cases a sub not a prime were the component manufacturers. Naturally, if you have a cooperative prime and you've done work for them in the past they will try to support you, but it's limited. When it gets to the user agency, we have had situations where the user agency says tell them to back off and that's the bottom line so we come see you.

A: Yes!

Don't forget that there's a difference between an item being a classified end item. It may not be. For instance, this microphone is not a classified end item. You can buy it in any microphone shop. But this is an exagerated example. It's use in a certain system or aboard a certain aircraft might be classified. The fact that I'm using this this way could be classified even though the end item itself is not. But the use might be classified. Or, it's relationship to something else might be classified. So you have to be careful there.

Q: Well, nothing we make would be considered an end use.

A: Yes. O.K.

Q: It would always have to be a component in a larger system.

A: Maybe the fact that that thing is a component is what's classified. And maybe that's why they're saying backoff.

Q: We could sell the same thing to a commercial account.

A: Yes, but they may not be using it the same way that this user agency is using it.

Q: But we don't have to know that in supplying it. In other words just give us the specification, boom, boom, boom.

A: That's true.

Q: All right. And it saves the taxpayer money by the way.

A: Yes, I see your point.

*EXERCISE #1*

**SITUATION #1:**

1. You are the Security Supervisor for the ABC Research T&E Company which has been awarded a prime contract by the Navy to produce SECRET classified hardware. ABC manufactures hardware but does not have the capability to produce the SECRET software program necessary to test the Remote Minehunting and Neutralization-Destruction System (REMINDS). Therefore, you decide to issue a subcontract to Software Development, Inc., FSC 12345, 1450 Juniper Street, Camden, NJ 08123. Your Purchase Order Number is X-14659. The work is to be completed one year from the effective date of the purchase order (one year from today's date).

2. Your review of the prime contract DD Form 254, (attached) reveals that item 11 is marked "YES" in subsections C, D, G, M and N. You determine the subcontractor will need to receive and generate classified documents to the level of SECRET, to include Restricted Data. You also determine the classification specifications and instructions for classifying the program and resulting documentation by the subcontractor will be in accordance with referenced guides (1), (2) and (5), under Section 15 of the prime contract DD Form 254.

**TASK #1:**

1. What actions are required by the ISM in connection with subcontracting?

2. Prepare the DD 254 for issue to Software Development, Inc., as a first tier subcontractor to your company.

3. Complete the following DD 254 items: 1, 2, 3 a & b, 4b, 5a, 7a, b, c, 8a, b, c, 10a, 11 (as appropriate), 12b, c, 13b, 14, 15, 16b thru e.

**SITUATION #2:**

1. You do not have the capability to store SECRET hardware at ABC Research. It is decided to construct a closed area, and you contact your IS Rep to discuss the requirements. The IS Rep explains the requirements of Section IV and App V, ISM.

2. Company management has agreed to hire a contract guard force to provide the required supplemental controls for storage of the hardware.

3. You negotiate with and finally contract with the Bluecoat Security Co., 2220 N. 22nd Street, Philadelphia PA 19108, to provide contract guard services.

**TASK #2:**

1. Complete the DD 254 to be issued to the Bluecoat Security Co. Fill in Blocks, 1, 2, 3, 4, 5, 7, 8 as appropriate, 10, 11, as appropriate, 12, 15 and 16.

2. What other considerations, if any, should you have concerning this subcontract?

**DEPARTMENT OF DEFENSE**
**CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: Secret

| 2. THIS SPECIFICATION IS FOR: | | 3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts) | 4. DATE TO BE COMPLETED (Estimated) | 5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a) | | | |
|---|---|---|---|---|---|---|---|
| X | a. PRIME CONTRACT | a. PRIME CONTRACT NUMBER N61331-82-C-0001 | a. 31 Dec 85 | X | a. ORIGINAL (Complete date in all cases) | | DATE 17 May 83 |
| | b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier) | b. FIRST TIER SUBCONTRACT NO. | b. | | b. REVISED (supersedes all previous specifications) | REVISION NO. | DATE |
| | c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION | c. IDENTIFICATION NUMBER | c. DUE DATE | | c. FINAL | | DATE |

6. Is this a follow-on contract? [ ] Yes [X] No If YES, complete the following:

a. _____ (PRECEDING CONTRACT NUMBER) b. _____ (DATE COMPLETED) c. Accountability for classified material on preceding contract

[ ] Is [ ] Is not transferred to this follow-on contract.

| 7a. Name, Address & Zip Code of Prime Contractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
|---|---|---|
| ABC Research T&E Co.<br>1234 N. 9th Street<br>Philadelphia, PA 19108 | 14365 | DIS/DIS, Philadelphia (S1411)<br>P.O. Box 13286<br>Philadelphia, PA 19101 |
| 8a. Name, Address & Zip Code of First Tier Subcontractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |
| 9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |

* When actual performance is at a location other than that specified, identify such other location in Item 15

| 10a. General identification of the Procurement for which this specification applies | b. DoDAAD Number of Procuring Activity identified in Item 16d |
|---|---|
| Fabricate and Test Remote Minehunting and Neutralization-Destruction System (REMINDS) | N61331 |

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [ ] Yes [X] No. If YES, identify the pertinent contractual documents in Item 15

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [ ] Yes [X] No. If YES, explain in Item 15 and identify specific areas or elements.

| 11. ACCESS REQUIREMENTS | YES | NO |
|---|---|---|
| a. Access to Classified Information Only at other contractor/Government activities. | | X |
| b. Receipt of classified documents or other material (for reference only (no generation)) | | X |
| c. Receipt and generation of classified documents or other material. | X | |
| d. Fabrication/Modification/Storage of classified hardware. | X | |
| e. Graphic arts services only. | | X |
| f. Access to IPO information. | | X |
| g. Access to RESTRICTED DATA | X | |
| h. Access to classified COMSEC information. | | X |
| i. Cryptographic Access Authorization required. | | X |

| ACCESS REQUIREMENTS (Continued) | YES | NO |
|---|---|---|
| j. Access to SENSITIVE COMPARTMENTED INFORMATION. | | X |
| k. Access to other Special Access Program Information (Specify in Item 15). | | X |
| l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories. | | X |
| m. Defense Documentation Center or Defense Information Analysis Center Services may be requested. | X | |
| n. Classified ADP processing will be involved. | X | |
| o. REMARKS: 11d: 25' X 12' area required. 11n: Word Processing System. | | |

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e)) EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official
Marylin H. Mifflin
MARYLIN H. MIFFLIN, HEAD
Information Security Div. (NCSC-361)

c. Activity name, address, Zip Code, telephone number and office symbol
Naval Coastal Systems Center
Panama City, FL 32407
(904)234-4396 AV: 436-4396

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.





DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

FOR TRAINING PURPOSES ONLY

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5a and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*:

Commanding Officer, Naval Coastal Systems Center (Code 101A), Panama City, FL 32407

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5a of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

[ ] a. A completed narrative is (1) [ ] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

[X] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [X] transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date)*.

[ ] c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.)*.

[ ] d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of _____.

[X] e. ~~Annual~~ Biennial review of this DD Form 254 is required. If "X'd", provide date such review is due: May 1985

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

The contractor will require access to background/reference material classified up to and including SECRET.
Ref:
14.b - Information generated under this contract will be classified in accordance with the guidance in the following:
(1) Unclassified enclosure (6) to OPNAVINST C5513.7A CH-2 dated 30 June 1980 (ID 07A-06.2) - refer to sections on the AN/SQQ-14 Deep Mod (now the AN/SQQ-30)
(2) Unclassified enclosure (13) to OPNAVINST C5513.7A CH-1 dated 25 Jan 1980 (ID 07A-13.1) - refer to sections on the MK 52 and MK 55 mines
(3) Unclassified enclosure (17) to OPNAVINST C5513.7A dated 9 Apr 1979 (ID 07A-17)
(4) Unclassified enclosure (18) to OPNAVINST C5513.7A CH-1 dated 25 Jan 1980 (ID 07A-18.1)
(5) Confidential enclosure (20) to OPNAVINST S5513.4A dated 1 Jun 1979 (ID 04A-20)
(6) Unclassified enclosure (67) to OPNAVINST S5513.4A dated 1 Jun 1979 (ID 04A-67)

All classified documents generated shall be marked in accordance with paragraph

(Continued)

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below

REQUIRED DISTRIBUTION:
- [X] Prime Contractor *(Item 7a)*
- [X] Cognizant Security Office *(Item 7c)*
- [X] Administrative Contracting Office *(Item 16e)*
- [X] Quality Assurance Representative
- [ ] Subcontractor *(Item 8a)*
- [ ] Cognizant Security Office *(Item 8c)*
- [ ] Program/Project Manager *(Item 12b)*
- [ ] U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:
- [X] NCSC: 723
- [X] 341
- [X] 361

b. Typed name and title of approving official
NATE SMITH
PCO

c. Signature
Nate Smith

d. Approving official's activity address and Zip Code
Naval Coastal Systems Center
Panama City, FL 32407

e. Name, address and Zip Code of Administrative Contracting Office
Conrad Hilton
DCASMA Philadelphia
P.O. Box 7478, Phila., PA 19101

GPO: 1982 0 — 505-101/82-3563

This is part of DD Form 254 dated 17 May 83 for Contract N61331-82-C-0001 with ABC Research T&E Company

---

Item 15. (continued)

11 of DoD 5220.22-M (current edition and changes thereto). Intelligence caveats, if any, required by the referenced security classification guides or when classifying derivately from source documents, shall be applied in paragraph markings and an overall document marking. The full intelligence caveat (e.g., NOT RELEASABLE TO FOREIGN NATIONALS) shall be placed at the bottom near the classification on the cover (if any), title page (if any), and the first page.

Classified information on this contract is not releasable to foreign nationals or personnel possessing "Reciprocal" clearance without the written approval of the Naval Coastal Systems Center (Code 360). The only exceptions to this requirement are a visit of a foreign national duly authorized by the Department of Defense through established channels or if authorized under the International Traffic in Arms Regulations.

Upon submission of the final end product on this contract, all classified material accountable to this contract shall be destroyed in accordance with paragraph 19 of DoD 5220.22-M, ISM; returned to the sender if so directed when transmitted, unless retention is requested and granted in accordance with paragraph 5.m of DoD 5220.22-M, or is authorized for transfer to a follow-on contract.

FOR TRAINING PURPOSES ONLY

Task #1

| DEPARTMENT OF DEFENSE<br>CONTRACT SECURITY CLASSIFICATION SPECIFICATION | 1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: _____ |
|---|---|

| 2. THIS SPECIFICATION IS FOR: | 3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER *(Prime contracts must be shown for all subcontracts)* | 4. DATE TO BE COMPLETED *(Estimated)* | 5. THIS SPECIFICATION IS: *(See "NOTE" below. If item b or c is "X'd", also enter date for item a)* | |
|---|---|---|---|---|
| a. PRIME CONTRACT | a. PRIME CONTRACT NUMBER | a. | a. ORIGINAL *(Complete date in all cases)* | DATE |
| b. SUBCONTRACT *(Use item 15 for subcontracting beyond second tier)* | b. FIRST TIER SUBCONTRACT NO. | b. | b. REVISED *(supersedes all previous specifications)* REVISION NO | DATE |
| c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION | c. IDENTIFICATION NUMBER | c. DUE DATE | c. FINAL | DATE |

6. Is this a follow-on contract? [ ] Yes [ ] No. If YES, complete the following:

a. _____ (PRECEDING CONTRACT NUMBER) b. _____ (DATE COMPLETED) c. Accountability for classified material on preceding contract

[ ] Is [ ] Is not, transferred to this follow-on contract.

| 7a. Name, Address & Zip Code of Prime Contractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
|---|---|---|
| 8a. Name, Address & Zip Code of First Tier Subcontractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| 9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |

* When actual performance is at a location other than that specified, identify such other location in Item 15

| 10a. General identification of the Procurement for which this specification applies | b. DoDAAD Number of Procuring Activity identified in Item 16d |
|---|---|

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [ ] Yes [ ] No. If YES, identify the pertinent contractual documents in Item 15.

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [ ] Yes [ ] No. If YES, explain in Item 15 and identify specific areas or elements.

| 11. ACCESS REQUIREMENTS | YES | NO | ACCESS REQUIREMENTS *(Continued)* | YES | NO |
|---|---|---|---|---|---|
| a. Access to Classified Information Only at other contractor/Government activities. | | | j. Access to SENSITIVE COMPARTMENTED INFORMATION. | | |
| b. Receipt of classified documents or other material *for reference only (no generation)* | | | k. Access to other Special Access Program Information *(Specify in Item 15).* | | |
| c. Receipt and generation of classified documents or other material. | | | l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories. | | |
| d. Fabrication/Modification/Storage of classified hardware. | | | m. Defense Documentation Center or Defense Information Analysis Center Services may be requested. | | |
| e. Graphic arts services only.. | | | n. Classified ADP processing will be involved. | | |
| f. Access to IPO Information. | | | o. REMARKS: | | |
| g. Access to RESTRICTED DATA. | | | | | |
| h. Access to classified COMSEC Information. | | | | | |
| i. Cryptographic Access Authorization required. | | | | | |

12. Refer all questions pertaining to contract security classification specification to the official named below *(NORMALLY, thru ACO (Item 16e)i EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).*

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

| b. Typed name, title and signature of program/project manager or other designated official | c. Activity name, address, Zip Code, telephone number and office symbol |
|---|---|
| | |

*NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.*



DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

**13a.** Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5a and Appendix IX)*.

**b.** Proposed public releases shall be submitted for approval prior to release ☐ Direct ☐ Through *(Specify)*:

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5a of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.*

**14.** Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)* Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☐ a. A completed narrative is (1) ☐ attached, or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached, or (2) ☐ transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date)*

☐ c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.)*.

☐ d. "X" only if this is a final specification and Item 5 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____.

☐ e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____.

**15.** Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

**16a.** Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the *User Agency* Contracting Officer or his Representative named in Item 16b below.

**REQUIRED DISTRIBUTION:**

- ☐ Prime Contractor *(Item 7a)*
- ☐ Cognizant Security Office *(Item 7c)*
- ☐ Administrative Contracting Office *(Item 16e)*
- ☐ Quality Assurance Representative
- ☐ Subcontractor *(Item 8a)*
- ☐ Cognizant Security Office *(Item 8c)*
- ☐ Program/Project Manager *(Item 12b)*
- ☐ U. S. Activity Responsible for Overseas Security Administration

**ADDITIONAL DISTRIBUTION:**

☐

☐

☐

b. Typed name and title of approving official

c. Signature

d. Approving official's activity address and Zip Code

e. Name, address and Zip Code of Administrative Contracting Office

* GPO 1982 0 — 505-101/82-3863

**DEPARTMENT OF DEFENSE**
**CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: _____

| 2. THIS SPECIFICATION IS FOR: | | 3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts) | 4. DATE TO BE COMPLETED (Estimated) | 5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a) | | |
|---|---|---|---|---|---|---|
| | a. PRIME CONTRACT | a. PRIME CONTRACT NUMBER | a. | | a. ORIGINAL (Complete date in all cases) | DATE |
| | b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier) | b. FIRST TIER SUBCONTRACT NO. | b. | | b. REVISED (supersedes all previous specifications) REVISION NO. | DATE |
| | c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION | c. IDENTIFICATION NUMBER | c. DUE DATE | | c. FINAL | DATE |

6. Is this a follow-on contract? [ ] Yes [ ] No. If YES, complete the following:

a. _____ (PRECEDING CONTRACT NUMBER) b. _____ (DATE COMPLETED) c. Accountability for classified material on preceding contract

[ ] Is [ ] Is not, transferred to this follow-on contract.

| 7a. Name, Address & Zip Code of Prime Contractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
|---|---|---|
| | | |
| 8a. Name, Address & Zip Code of First Tier Subcontractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |
| 9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |

* When actual performance is at a location other than that specified, identify such other location in Item 15

| 10a. General identification of the Procurement for which this specification applies | b. DoDAAD Number of Procuring Activity identified in Item 16d |
|---|---|
| | |

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [ ] Yes [ ] No. If YES, identify the pertinent contractual documents in Item 15

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [ ] Yes [ ] No. If YES, explain in Item 15 and identify specific areas or elements.

| 11 ACCESS REQUIREMENTS | YES | NO | ACCESS REQUIREMENTS (Continued) | YES | NO |
|---|---|---|---|---|---|
| a. Access to Classified Information Only at other contractor/Government activities. | | | j. Access to SENSITIVE COMPARTMENTED INFORMATION. | | |
| b. Receipt of classified documents or other material for reference only (no generation) | | | k. Access to other Special Access Program information (Specify in Item 15). | | |
| c. Receipt and generation of classified documents or other material. | | | l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories. | | |
| d. Fabrication/Modification/Storage of classified hardware. | | | m. Defense Documentation Center or Defense Information Analysis Center Services may be requested. | | |
| e. Graphic arts services only. | | | n. Classified ADP processing will be involved. | | |
| f. Access to IPO information. | | | o. REMARKS: | | |
| g. Access to RESTRICTED DATA. | | | | | |
| h. Access to classified COMSEC information. | | | | | |
| i. Cryptographic Access Authorization required. | | | | | |

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

| b. Typed name, title and signature of program/project manager or other designated official | c. Activity name, address, Zip Code, telephone number and office symbol |
|---|---|
| | |

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.



DD FORM 1 JAN 79 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254, WHICH IS OBSOLETE

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5o and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release [ ] Direct [ ] Through *(Specify)*:

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5o of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5o, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

[ ] a. A completed narrative is (1) [ ] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

[ ] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [ ] transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date)*.

[ ] c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.)*.

[ ] d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____

[ ] e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below

**REQUIRED DISTRIBUTION:**

[ ] Prime Contractor *(Item 7a)*
[ ] Cognizant Security Office *(Item 7c)*
[ ] Administrative Contracting Office *(Item 16e)*
[ ] Quality Assurance Representative
[ ] Subcontractor *(Item 8a)*
[ ] Cognizant Security Office *(Item 8c)*
[ ] Program/Project Manager *(Item 12b)*
[ ] U. S. Activity Responsible for Overseas Security Administration

**ADDITIONAL DISTRIBUTION:**

[ ]
[ ]

b. Typed name and title of approving official

c. Signature

d. Approving official's activity address and Zip Code

e. Name, address and Zip Code of Administrative Contracting Office

FOR TRAINING PURPOSES ONLY Solution Task #1

**DEPARTMENT OF DEFENSE**
**CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: Secret

| 2. THIS SPECIFICATION IS FOR: | | 3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts) | 4. DATE TO BE COMPLETED (Estimated) | 5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a) | | |
|---|---|---|---|---|---|---|
| | a. PRIME CONTRACT | a. PRIME CONTRACT NUMBER N61331-82-C-0001 | a. | X | a. ORIGINAL (Complete date in all cases) | DATE 22 Jun 83 |
| X | b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier) | b. FIRST TIER SUBCONTRACT NO. X-14659 | b. 21 Jun 84 | | b. REVISED (supersedes all previous specifications) REVISION NO. | DATE |
| | c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION | c. IDENTIFICATION NUMBER | c. DUE DATE | | c. FINAL | DATE |

6. Is this a follow-on contract? ☐ Yes ☒ No. If YES, complete the following:
a. _____ (PRECEDING CONTRACT NUMBER) b. _____ (DATE COMPLETED) c. Accountability for classified material on preceding contract
☐ Is ☐ Is not, transferred to this follow-on contract.

| 7a. Name, Address & Zip Code of Prime Contractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
|---|---|---|
| ABC Research T&E Company<br>1234 N. 9th Street<br>Phila., PA 19108 | 14365 | DIS/DIS, Phila. (S1411)<br>P.O. Box 13286<br>Phila., PA 19101 |
| 8a. Name, Address & Zip Code of First Tier Subcontractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| Software Development, Inc.<br>1450 Juniper St.<br>Camden, NJ 08123 | 12345 | (Same) |
| 9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |

* When actual performance is at a location other than that specified, identify such other location in Item 15

10a. General identification of the Procurement for which this specification applies: Software development program for REMINDS

b. DoDAAD Number of Procuring Activity identified in Item 16d: N/A

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? ☐ Yes ☒ No. If YES, identify the pertinent contractual documents in Item 15

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? ☐ Yes ☒ No. If YES, explain in Item 15 and identify specific areas or elements.

| 11. ACCESS REQUIREMENTS | YES | NO |
|---|---|---|
| a. Access to Classified Information Only at other contractor/Government activities. | | X |
| b. Receipt of classified documents or other material for reference only (no generation) | | X |
| c. Receipt and generation of classified documents or other material. | X | |
| d. Fabrication/Modification/Storage of classified hardware. | | X |
| e. Graphic arts services only. | | X |
| f. Access to IPO information. | | X |
| g. Access to RESTRICTED DATA. | X | |
| h. Access to classified COMSEC information. | | X |
| i. Cryptographic Access Authorization required. | | X |

| ACCESS REQUIREMENTS (Continued) | YES | NO |
|---|---|---|
| j. Access to SENSITIVE COMPARTMENTED INFORMATION. | | X |
| k. Access to other Special Access Program Information (Specify in item 15). | | X |
| l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories. | | X |
| n. Defense Documentation Center or Defense Information Analysis Center Services may be requested. | | X |
| n. Classified ADP processing will be involved. | X | |
| o. REMARKS: | | |

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official
I. M. Ceekure
Security Officer
I. M. Ceekure

c. Activity name, address, Zip Code, telephone number and office symbol
ABC Research T&E Company
1234 N. 9th Street
Philadelphia, PA 19108 (215)952-1234

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5o and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*:

Individual named in Item 12 b and c.

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5o of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5o, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

[ ] a. A completed narrative is (1) [ ] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

[X] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [X] transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date).*

[ ] c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.)*.

[ ] d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of _____.

[X] e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: Biennial N/A.

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

Item 14b: Information generated under this contract will be classified in accordance with the guidance in the following:

(1) Unclassified enclosure (6) to OPNAVINST C5513.7A, CH-2, 30 Jun 80- refer to sections on the AN/SQQ 14 Deep Mod (now the AN/SQQ-30)
(2) Unclassified enclosure (13) to OPNAVINST C5513.7.A, CH-1, 25 Jan 80- refer to sections on the MK52 and MK55 mines
(3) Confidential enclosure (20) to OPNAVINST S55.134A. 1 Jun 79

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below

REQUIRED DISTRIBUTION:

[X] Prime Contractor *(Item 7a)*
[ ] Cognizant Security Office *(Item 7c)*
[X] Administrative Contracting Office *(Item 16e)*
[X] Quality Assurance Representative
[X] Subcontractor *(Item 8a)*
[X] Cognizant Security Office *(Item 8c)*
[X] Program/Project Manager *(Item 12b)*
[ ] U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

b. Typed name and title of approving official
CONRAD HILTON
Administrative Contracting Officer

c. Signature
Conrad Hilton

d. Approving official's activity address and Zip Code
DCASMA, Philadelphia
P.O. Box 7494
Philadelphia, PA 19101

e. Name, address and Zip Code of Administrative Contracting Office
Same as b and d above

FOR TRAINING PURPOSES ONLY Solution Task #2

**DEPARTMENT OF DEFENSE**
**CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: Secret

| 2. THIS SPECIFICATION IS FOR: | | 3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts) | 4. DATE TO BE COMPLETED (Estimated) | 5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a) | | |
|---|---|---|---|---|---|---|
| | a. PRIME CONTRACT | a. PRIME CONTRACT NUMBER N61331-82-C-0001 | a. | X | a. ORIGINAL (Complete date in all cases) | DATE 22 Jun 83 |
| X | b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier) | b. FIRST TIER SUBCONTRACT NO. P.O. 12345 | b. 31 Dec 83 | | b. REVISED (supersedes all previous specifications) REVISION NO. | DATE |
| | c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION | c. IDENTIFICATION NUMBER | c. DUE DATE | | c. FINAL | DATE |

6. Is this a follow-on contract? [ ] Yes [X] No If YES, complete the following:
a. _____ (PRECEDING CONTRACT NUMBER) b. _____ (DATE COMPLETED) c. Accountability for classified material on preceding contract
[ ] Is [ ] Is not, transferred to this follow-on contract.

| 7a. Name, Address & Zip Code of Prime Contractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
|---|---|---|
| ABC Research T&E Company<br>1234 N. 9th St.<br>Phila., PA 19108 | 14365 | DIS/DIS, Phila. (S1411)<br>P.O. Box 13286<br>Phila., PA 19101 |
| 8a. Name, Address & Zip Code of First Tier Subcontractor * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| Bluecoat Security Co.<br>2220 N. 22nd St.<br>Phila., PA 19108 | 5A190 | Same |
| 9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ * | b. FSC Number | c. Name, Address & Zip Code of Cognizant Security Office |
| | | |

* When actual performance is at a location other than that specified, identify such other location in Item 15

10a. General identification of the Procurement for which this specification applies: Guard Service
b. DoDAAD Number of Procuring Activity identified in Item 16d.

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [ ] Yes [X] No. If YES, identify the pertinent contractual documents in Item 15

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [ ] Yes [X] No. If YES, explain in Item 15 and identify specific areas or elements.

| 11. ACCESS REQUIREMENTS | YES | NO | ACCESS REQUIREMENTS (Continued) | YES | NO |
|---|---|---|---|---|---|
| a. Access to Classified Information Only at other contractor/Government activities. | X | | j. Access to SENSITIVE COMPARTMENTED INFORMATION. | | X |
| b. Receipt of classified documents or other material for reference only (no generation) | | X | k. Access to other Special Access Program Information (Specify in item 15). | | X |
| c. Receipt and generation of classified documents or other material. | | X | l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories. | | X |
| d. Fabrication/Modification/Storage of classified hardware. | | X | m. Defense Documentation Center or Defense Information Analysis Center Services may be requested. | | X |
| e. Graphic arts services only. | | X | n. Classified ADP processing will be involved. | | X |
| f. Access to IPO information. | | X | o. REMARKS: | | |
| g. Access to RESTRICTED DATA. | | X | | | |
| h. Access to classified COMSEC information. | | X | | | |
| i. Cryptographic Access Authorization required. | | X | | | |

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official: See Item 16

c. Activity name, address, Zip Code, telephone number and office symbol

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.



DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

13a. Information pertaining to classified contracts or projects even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5a and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*:

See Item 16

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5a of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

[ ] a. A completed narrative is (1) [ ] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

[ ] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [ ] transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date)*.

[X] c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.)*.

* [ ] d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____

[ ] e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

Actual knowledge of, generation, or production of classified NOT REQUIRED. This document serves as written notice of the letting of a classified service contract. The highest level of classification for the contract is SECRET.

(See Paragraph 60h(1)(b), ISM)

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below

**REQUIRED DISTRIBUTION:**

- [ ] Prime Contractor *(Item 7a)*
  - [ ] Cognizant Security Office *(Item 7c)*
- [ ] Administrative Contracting Office *(Item 16e)*
  - [ ] Quality Assurance Representative
- [ ] Subcontractor *(Item 8a)*
  - [ ] Cognizant Security Office *(Item 8c)*
- [ ] Program/Project Manager *(Item 12b)*
  - [ ] U. S. Activity Responsible for Overseas Security Administration

**ADDITIONAL DISTRIBUTION:**

[ ]
[ ]
[ ]

b. Typed name and title of approving official

I. M. CEEKURE, Security Officer

c. Signature

I. M. Ceekure

d. Approving official's activity address and Zip Code

ABC Research IGE Company
1234 N. 9th St.
Phila., PA 19108 (215)952-1234

e. Name, address and Zip Code of Administrative Contracting Office

0183

## INSTRUCTIONS FOR COMPLETING PRIME CONTRACT DD 254

The following instructions apply to the item numbers on the DD Form 254.

Item 1 — Insert the highest level of clearance required for access to classified information in the performance of the contract. Use only the word TOP SECRET, SECRET, or CONFIDENTIAL. Special caveats such as RESTRICTED DATA, FORMELY RESTRICTED DATA, CRYPTOGRAPHIC INFORMATION, etc, should *not* be indicated in the Item 1 block. The facility security clearance of the contractor must be at least as high as the classification indicated in this block.

Item 2 — Check Item 2a for prime contracts. Item 2c for RFQ, RFP, IFP, etc., as applicable.

Item 3 — Enter in Item 3a the prime contract identification number (PIIN). The identification number (PIIN), of RFQ, RFB, IFQ, IFB, etc. will be entered in Item 3c.

Item 4 — For the procurement action identified in Item 3, enter the estimated date on which the procurement action is to be completed. Completion dates for RFQs, etc. will be the due date for the bid or quote.

Item 5 — Pertains only to the DD Form 254 being prepared. Enter an X in the left-hand column of Item 5 to indicate whether it is an original, revised, or final DD Form 254. In the right-hand column, enter the date of the DD Form 254 being issued.

Note: The date of the original DD Form 254 (Item 5a) will appear unchanged on each revised and final DD Form 254. Each time a DD Form 254 is revised, it will be given a revision number. A final DD 254 is only issued when remaining classified material is declassified, or when retention is authorized. (Para. 7-102b, ISR)

Item 6 — Pertains to follow-on contracts and to contracts awarded to a successful bidder on an RFQ, RFP, etc. The follow-on contract must be to the same contractor for the same item(s) or service(s), with no changes in the security classification guidance applicable to the prime contract. A contract awarded to a successful bidder must be the direct result of an RFQ, RFP, etc., with no changes in the security classification guidance applicable to the RFQ, RFP, etc. and the contract. When these conditions apply, enter an X in the "Yes" box, and enter the number and completion date of the preceding prime contract or the RFQ in Items 6a and 6b. In Item 6c, enter an X in the "Is" box. In all other cases, enter an X in the "No" box. This is a very important change, as it authorizes automatic retention of residual classified documents pertaining to the completed prime contract or RFP, and will eliminate much administrative effort.

Item 7 — In Item 7a, enter the name and address of the prime contractor. The name and address entered in Item 7a must be identical to that furnished by the cognizant security office of the facility named in Item 7c. Normally, these will be DIS Regions. In Item 7b enter the FSC number for the facility named in Item 7a. The FSC number is the Federal Supply Code number of the facility. This number will be furnished on request by the DIS cognizant office. The asterisk (*) that appears in Item 7a is a reference to the footnote that extends across the foot of the blocks.

Item 10 — In Item 10a, enter the item(s) being procured under the contract. This may be material, studies, services, etc. The statement should be short, concise, and unclassified. Item 10b is the Department of Defense Activities Address Directory Code number. Item 10c indicates whether or not the program requires security measures that are additional to those normally required to the Industrial Security Program, such as special access programs. Item 10d indicates whether part or all of the work performed on the contract will be inspected by an agency other than the facility's cognizant security

office. If so, this represents a "carve out" and requires Secretary or Under-secretary approval of the Military Department.

Item 11a through 11o Definitions:

Item 11a — Access to Classified Information only at other contractor/government facilities. Note the word "only." If the YES box is marked for this item, the NO box in each of Items 11b through 11e plus 11m and 11n *must* be marked and the remaining items marked as required.

Item 11b — Receipt of classified documents or other material for reference only (no generation). Note the word "only." If the YES box is marked for this item, the NO box in each of Items 11a, 11c through 11e, and 11n must be marked and the remaining items marked as required.

Item 11c — Receipt and generation of classified documents or other material. If the YES box is marked for this item, the NO box in each of Items 11a, 11b, and 11e must be marked and the remaining items marked as required.

Item 11d — Fabrication/Modification/Storage of classified hardware. Same as Item 11c.

Item 11e — Graphic Arts Services only. Note the word "only." If the YES box is marked for this item, the NO box in each of the items 11a through 11d must be marked and the remaining items marked as required.

Item 11f — Access to IPO information. IPO means International Pact Organizations such as NATO, CENTO, SALT Talks, etc.

Item 11g — Access to RESTRICTED DATA. This includes access to FORMERLY RESTRICTED DATA and CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) and is information developed and controlled under the Atomic Energy Act of 1954.

Item 11h — Access to classified COMSEC information. This is communications security information.

Item 11i — Cryptographic Access Authorization required. This access requires access to operational keys, codes, and ciphers for cryptographic equipment. Special security clearances and briefings are required.

Item 11j — Access to SENSITIVE COMPARTMENTED INFORMATION

Item 11k — Access to other Special Access Program information. Normally, these type of programs require additional security procedures or actions. These requirements are varied and may be different for each type of special access program.

Item 11l — Access to U.S. classified information outside of the U.S. Panama Canal Zone, Puerto Rico, U.S. Possessions and Trust Territories.

Item 11m — Defense Technical Information Center services may be requested.

Item 11n — Classified ADP processing will be involved at the prime contractor's facility. This requires approved ADP system per Section XIII, ISM.

Item 11o — REMARKS. This block may be used for other instructions by the User Agency.

Item 12 — Note that Item 12a is a statement of completeness and adequacy of the DD Form 254 that is being signed by the individual named in Item 12b. Item 12b contains the typed name and signature of the person who can interpret the classified requirements of the contract. Item 12c contains the complete mailing address and telephone number including Autovon of the individual named in Item 12b. Inquiries pertaining to classification guidance, determinations or interpretations shall be directed to this official.

Item 13 — Normally, proposed public releases should be submitted through the User Agency Public Information Office.

Item 14 — Item 14a and 14b specify the type(s) of security classification guidance furnished for use in the performance of the prime contract. Item 14c indicates that it is a service-type contract and will be checked if Item 11a is "Yes." If Items 14a and/or 14b are used, Item 14c will not be used and vice versa. Item 14d pertains to the retention of residual classified material after contract completion and this would be a Final DD 254. Item 14e should read "Biennial review. . . etc." in conformance with E.O. 12065, and DoD 5200.1R. Service type contracts (Item 11a) do not require biennial review. There are various ways by which a prime contractor may be furnished security classification guidance: 1) a narrative style classification guide prepared from various sources; 2) User agency security classification guides or extracts or portions there of; and 3) a combination of 1) and 2). Item 14a will be marked whenever a narrative guide is prepared by the issuing activity. This narrative may be placed in Item 15 or on an attached sheet, or a combination of both. This narrative will be attached unless it is classified. Item 14b will be used whenever the prime contractor is furnished User Agency security classification guides or extracts or portions thereof. These guides will be attached unless they are classified.

Item 15 — The purpose of this block is to provide the contractor with the security classification guidance required for prime contract performance. The classification guidance will normally include one or more of the following:

*1* Identification of security classifications guides or extracts thereof furnished by the User Agency or identification of specific documents from which classification guidance may be obtained.
*2* Narrative classification guidance, prepared by the issuer which identifies the specific types of information to be classified and appropriate downgrading and declassification instructions. When classified hardware is a part of the procurement, the narrative guide must identify each item of classified hardware.
*3* Special instructions and controls for the handling, processing, storing, and transmission of classified information and material. Included are explanatory comments required for information on activities identified in Items 10 and 11 and/or supplements to the classification guidance indicated in *1* and *2* above.
*4* When the prime contract is for certain types of services and Item 14c is marked, specific statements must appear in Item 15. These statements are contained in Paragraph 7.102d(4), ISR.

Item 16 — Block 16 indicates the name and address of the User Agency contracting officer or his representative who approves the DD Form 254. Distribution should be marked to conform with Paragraph 7-103, ISR.

## INSTRUCTIONS FOR COMPLETING SUB-CONTRACT DD 254

The following instructions apply to the item numbers on the DD Form 254.

Item 1 — Insert the highest level of clearance required for access to classified information in the performance of the contract. Use only the word TOP SECRET, SECRET, or CONFIDENTIAL. Special caveats such as RESTRICTED DATA, FORMERLY RESTRICTED DATA, CRYPTOGRAPHIC INFORMATION, etc., should *not* be indicated in the Item 1 block. The facility security clearance of the subcontractor must be at least as high as the classification indicated in this block. The classification indicated in this block can be no higher than the classification indicated in the same block on the DD Form 254 for the prime contract under which the subcontract is being awarded.

Item 2 — Check Item 2b for subcontracts or Item 2c for RFQ, RFP, IFB, etc., as applicable.

Item 3 — Enter in Item 3a the prime contract identification number. The identification number of any subcontract or RFQ being issued will be entered in Item 3b (subcontract) or 3c (RFQ). When subcontract is second tier (contract or RFQ), enter in Item 3a the prime contract (RFQ) identification number; enter in Item 3b or 3c, as applicable, the identification number of the subcontract or RFQ under which subcontractor is performing; enter in Item 9a (or in Item 15) the identification number of the 2nd tier subcontract or RFQ being issued.

Item 4 — For each procurement action identified in items 3, 9, and 15, or on a continuation sheet, enter the estimated date on which the procurement action is to be completed. Beginning with Item 4a, each lower level completion date must be less than (or no more than equal to) the one above. Completion dates for RFQs will be the due date and will be less than (or no more than equal to) the one above.

Item 5 — The information in the Item 5 block pertains only to the DD Form 254 being prepared. Enter an X in the left-hand column of Item 5 to indicate whether it is an original, revised, or final DD Form 254. In the right hand column, enter the date of the DD Form 254 being issued.

Note: The date of the original DD Form 254 (Item 5a) will appear unchanged on each revised and final DD Form 254. Each time a DD Form 254 is revised, it wiil be given a revision number. A final DD 254 is only issued when remaining classified material is declassified; or when retention is authorized, and are not normally issued by Prime Contractors.

Item 6 — This block pertains to follow-on contracts and to contracts awarded to a successful bidder on an RFQ. The follow-on contract must be to the same subcontractor for the same item(s) or service(s), with no changes in the security classification guidance applicable to the subcontract. A contract awarded to a successful bidder must be the direct result of an RFQ, with no changes in the security classification guidance applicable to the RFQ and the subcontract. When these conditions apply, enter an X in the "Yes" box, and enter the number and completion date of the preceding subcontract or the RFQ in Items 6a and 6b. In Item 6c, enter an X in the "Is" box. In all other cases, enter an X in the "No" box. This is a very important change, as it authorizes automatic retention of residual classified documents pertaining to the completed subcontract or RFQ, and will eliminate much administrative effort.

Item 7, 8, and 9 — In Item 7a, enter the name and address of the prime contractor, in Item 8a, the name and address of the first tier subcontractor, and in Item 9as, the name and address of the second tier subcontractor. the names and addresses entered in Items 7a, 8a, and 9a must be identical to those furnished by the cognizant security offices of the facilities who are named in Items 7c, 8c and 9c, normally, these will be DIS Regions.

In Items 7b, 8b, and 9b, enter the FSC numbers for the facilities named in Items 7a, 7b, and 7c. The FSC number is the Federal Supply Code number of the facility, which will be furnished, on request, by the DIS cognizant office. For subcontracting beyond the second tier, show similar information for each successive tier in Item 15 or on a DD Form 254 continuation sheet. The asterisk (*) that appears in each block of Items 7a, 8a, and 9a is a reference to the footnote that extends across the foot of the blocks.

Item 10 — In Item 10a, enter the item(s) being procured under the contract. This may be material, studies, services, etc. The statement should be short, concise, and unclassified. Item 10b is the Department of Defense Activities Address Directory. For DD Forms 254 issued on subcontracts, this block will *always* be marked N/A (not applicable). Item 10c indicates whether or not the program requires security measures that are additional to those normally required in the Industrial Security Program, such as special access programs. Item 10d indicates whether part or all of the work performed on the contract will be inspected by an agency other than the facility's cognizant security office. A "Yes" indicated for 10c and 10d must be approved by the ACO/PCO.

Items 11a through 11o Definitions:

Item 11a — Access to Classified Information only at other contractor/government facilities. Note the word "only." If the YES box is marked for this item, the NO box in each of Items 11b through 11e plus 11m and 11n *must* be marked and the remaining items marked as required.

Item 11b — Receipt of classified documents or other material for reference only (no generation). Note the word "only." If the YES box is marked for this item, the NO box in each of Items 11a, 11c through 11e, and 11n must be marked and the remaining items marked as required.

Item 11c — Receipt and generation of classified documents or other material. If the YES box is marked for this item, the NO box in each of Items 11a, 11b, and 11c must be marked and the remaining items marked as required.

Item 11d — Fabrication/Modification/Storage of classified hardware. Same as Item 11c.

Item 11e — Graphic Arts Services only. Note the word "only." If the YES box is marked for this item, the NO box in each of the items 11a through 11d must be marked and the remaining items marked as required.

Item 11f — Access to IPO information. IPO means International Pact Organizations such as NATO, CENTO, SALT Talks, etc.

Item 11g — Access to RESTRICTED DATA. This includes access to FORMERLY RESTRICTED DATA and CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) and is information developed and controlled under the Atomic Energy Act of 1954.

Item 11h — Access to classified COMSEC information. This is communications security information. Permission of the prime contracting officer is required prior to subcontracting.

Item 11i — Cryptographic Access Authorization required. This access requires access to operational keys, codes, and ciphers for cryptographic equipment. Special security clearances and briefings are required. Permission of the prime contracting officer is required prior to subcontracting.

Item 11j — Access to SENSITIVE COMPARTMENTED INFORMATION. For subcontracts, contact the ACO/PCO.

Item 11k — Access to other Special Access Program information. Normally, these type of programs require additional security procedures or actions. These requirements are varied and may be different for each type of special access program.

Item 11l — Access to U.S. classified information outside of the U.S. Panama Canal Zone, Puerto Rico, U.S. Possessions and Trust Territories.

Item 11m — Defense Technical Information Center services may be requested.

Item 11n — Classified ADP processing will be involved at the subcontractor facility. This requires approved ADP system per Section XIII, ISM.

Item 11o — REMARKS. This block may be used for other specific instructions.

Item 12 — In subcontracting situations, item 12 will contain the signature and typed name and title of the security supervisor of the facility issuing the subcontract. Inquiries pertaining to classification guidance, determinations or interpretations shall be directed to this official.

Item 13 — Public releases will normally be cleared by the authority indicated in Item 13 of the prime contract DD Form 254.

Item 14 — Items 14a and 14b specify the type(s) of security classification guidance furnished for use in the performance of the subcontract. Item 14c indicates that the subcontract is a service-type contract and Item 11a must be marked "Yes." If Items 14a and/or 14b are used, Item 14c will not be used and vice versa. When Item 14c is used the approving authority for the DD Form 254, Items 16b, 16c and 16d will be a company representative. Item 14d pertains to the retention of residual classified material after subcontract completion and are normally not checked by Prime Contractors. Item 14e should read "Biennial review. . . etc." in conformance with E.O. 12065. There are various ways by which a subcontract or may be furnished security classification guidance: 1) a narrative-style classification guide prepared from various sources; 2) User Agency security classification guides or extracts or portions thereof; and 3) a combination of 1) and 2). Item 14a will be marked whenever a narrative guide is prepared by the issuing activity. This narrative may be placed in Item 15 or on an attached sheet, or a combination of both. The narrative will be attached unless it is classified. Item 14b will be used whenever the subcontractor is furnished User Agency security classification guides or extracts or portions thereof. These guides will be attached unless they are classified.

Item 15 — The purpose of this block is to provide the subcontractor with the security classification guidance required for subcontract performance. The classification guidance will normally include one or more of the following:

1 Identification of security classification guides or extracts thereof furnished to the issuer by the User Agency or prime contractor; or identification of specific documents from which classification guidance may be obtained.
2 Narrative classification guidance, prepared by the issuer which identifies the specific types of information to be classified and appropriate downgrading and declassification instructions. When classified hardware is a part of the procurement, the narrative guide must identify each item of classified hardware.

*3* Special instructions and controls for the handling, processing, storing, and transmission of classified information and material. Included are explanatory comments required for information on activities identified in Items 10 and 11 and/or supplements to the classification guidance indicated in *1* and *2* above.

*4* When the subcontract is for services and Item 14c is marked, specific statements must appear in Item 15. These statements are contained in paragraph 60h, ISM.

Item 16 — Block 16 indicates the name and address of the User Agency contracting officer or his representative or contractor official who approves the DD Form 254. Distribution should be marked to conform with para. 61, ISM.

*PANEL*
*OPSEC WHERE ARE WE???*

**Elmer Hargis**
**Ballistics Missile Command**
**Huntsville, Alabama**

I saw the program, I looked and said, "Hey, what's this thing called 'OPSEC — Where Are We!'" Then I saw three big question marks. I wondered what Jerry had in mind and he mentioned a little bit there, and I've had other questions along the road. Irv Boker said "Hey, we need to find out what OPSEC is all about and we want to see where we are." You ought to do a little effectiveness review of how well OPSEC is doing in industry.

I'm not going to tell you how to do OPSEC today. I've written the book on it. Here it is. I left six autographed copies in the back. If you want additional copies, we have them available, for $29.95. No really, we do have some good information how to do OPSEC in a contractor community. If you'd like a copy of this, give Bill Johnson, whose handling the viewgraph transparencies for me, your name and where to send it or write us or give me your desires, and we'll try help you with it.

I welcome the opportunity to be here with you today and to give you an update on the industrial security operation program for the Army Ballistic Missile Defense Organization.

In addition, I would like to briefly describe the current BMD program. At least what was current when we left Huntsville. I also talked about the BMD program in my presentation last May. Since then, virtually everything I told you has changed.

Research and development now places greater emphasis on what we're doing much more than the specific systems that we were talking about last year. Such changes as this is not unusual in the BMD business.

The fundamental technologies required to solve the BMD program, however, remain relatively constant.

President Reagan has supported BMD, of course, in his speech to the nation on the 25th of March. The President presented the benefits from a strategic program against ballistic missiles. The bottom line is that with such defense, people can live secure in the knowledge that our lives are not threatened by nuclear missiles.

You may ask, how did BMD and industrial OPSEC get involved with each other? In other words, what is a nice program like BMD doing in the OPSEC business?

General Vessey was being briefed by our program manager and he discussed the need for broader involvement by the Army staff in the BMD program. He expressed considerable concern about the loss of technology to the Soviets. General Vessey, who was then Vice Chief of Staff of the Army, and is today the Chief of Staff focused on OPSEC. He made these points: That the program may mean overall survival of the United States. The BMD program should not be compromised through poor OPSEC. He said "what do we want the Soviets to know about the BMD and what do we not want the Soviets to know about BMD?" He said "I want the Deputy Chief of Staff for Operation and other agencies, the office of the Assistant Chief of Staff for Intelligence and the BMD organization to conduct an OPSEC study and set up requirements where we can put OPSEC into outside agencies such as the Air Force, OSD and contractors to make sure that we don't compromise BMD through poor OPSEC."

We developed a plan. The plan integrates all of the headquarters of the Department of Army staff agencies and Army commands under an OPSEC umbrella. It emphasizes protection of operations, tests and activities to ensure that we have proper procedures that we don't compromise what we're doing. The plan emphasizes practical counter measures, cost effective counter measures, and it establishes a base for coordination of the BMD OPSEC activities within the Department of Energy and other outside agencies.

General Vessey also sent a letter to major Commanders stating, and I want to quote from that message, "The BMD program is of vital importance to the security of the United States. The Army is totally committed to improving OPSEC Army wide and especially OPSEC as it relates to the BMD program. The importance of this pro-

gram cannot be overemphasized and I solicit your total support."

This has been able to get the commands to give us the necessary support for OPSEC. Now the plan that we developed is to compliment the Defense Investigative Service Program, it's not to replace the DIS Program. Again let me tell you that it emphasizes protection of operations, test and experimental activities. The plan emphasizes practical fixes and provisions for requests for waivers and are provided when the OPSEC analysis indicates that a waiver should be obtained. The plan sets up procedures for coordination and establishes a vehicle for obtaining support in other organizations that are involved in the BMD work.

I'd like to talk about some of our program accomplishments. It's the intent of the BMD OPSEC program to limit to the greatest degree that we can, the capability of hostile intelligence to gain critical information concerning BMD research and development. We've made significant progress in implementing OPSEC in the BMD community. The intelligence and security command or primarily the 902nd Military Intelligence Group, have provided threat briefings to 75 BMD contractors. We currently have 57 contractor OPSEC plans that have been approved for use in the contractor program.

The contractors identified (through the OPSEC analysis process) several critical items involving BMD technology which would be subseptible to hostile intelligence collection. Some exciting things happened as the contractors looked at their program.

Classified work in one facility was being done on four different word processors. These are examples of what we found. Two of the machines that the contractor was using had been TEMPEST approved, and they'd been primarily purchased to do work for a SCIF. But the other two machines were not TEMPEST approved. The contractor, through OPSEC analysis, recognized that here is a problem that I can do something about. He started using the TEMPEST approved machines for all of his classified work and BMD information, and used the unprotected machines for other types of work. So this was an improved security procedure without any additional cost.

In the book destruction of test data, one of our major contractors was doing testing and a lot of photography. He had a large vault full of unclassified material. When he looked at it from an OPSEC standpoint, the compiliation of that material would give away classified information. He realized that it would require a lot of effort on the part of his technical people to go through all of that material and to try to sort out the classified information to be protected. He decided that the proper approach would be to destroy the whole vault full of material. This was done and it certainly was an improvement.

Systematic analysis of software, as far as we know, has not been done in the past with a major contractor. This is looking at the software to determine what needs to be protected in the way of computer software. Along with that analysis of the software, he is also looking at the probability of being able to segregate the classified software and information into an area that he can provide better protection for. This is probably the first time that security has been a prime consideration in trying to look at software operations by our computer people. And certainly to modify programs to accomodate security.

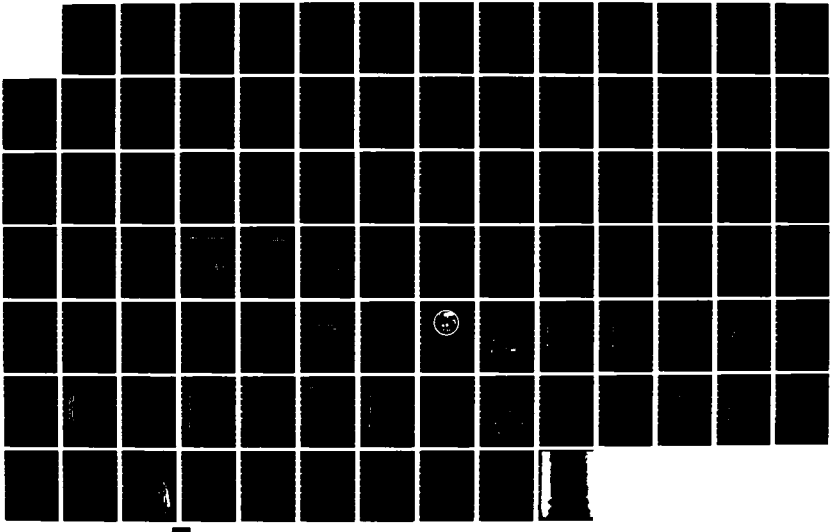
Through OPSEC, security has been included in the main stream of the Weapon System Development Program that we have.

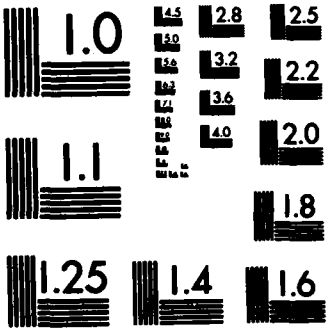
Prior to OPSEC, security was generally regarded as a compliance program that was enforced by the government. Under OPSEC, the contractor that we've dealt with has been showing initiative in identifying problems and recommending solutions to those problems. I think of even more importance, the contractor has assumed responsibility as an active participant in the program. W.B.S. stands for work breakdown structure. This is to identify the funding that is required for implementing OPSEC and this is included in the contractors costing. We include the OPSEC plan as part of the contract deliverables. And, of course, the last part of that is that at our major milestone reviews, one of the items to be reviewed is the OPSEC program and the status of that by the contractor.

The cumulative sensitivity of the contractors operation is beginning to be recognized by the

AD-A143 015 CLASSIFICATION MANAGEMENT JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY VOLUME 19 1983(U) NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ROCKVILLE MD 2/2

UNCLASSIFIED E SUTO ET AL. 1984 F/G 5/2 NL





contractor's personnel. The OPSEC plans are identifying vulnerabilities that have gone previously unnoticed. For example, the external views of some hardware is not indicative of classified information by itself. But when you take that external view and combine it with all the other information in the public domain, which was put there through open sources, this does give information in many cases that would enable hostile intelligence to derive classified information.

Also, our contractors are realizing the sensitivity of laboratory tests. Tests involving hardware in the loops. They are now aware that the test results of a small component of a missile can reveal just as much as a flight test of the completed system.

Another item was the encription of telimetry during flight tests. This represents another achievement. Encription of telimeters is something we've talked about for a long time, in the missile business especially, but we haven't done a lot about it. Through the momentum of our OPSEC program, we were able to get crypto equipment and change our designs to include it and do necessary coordination to protect the stream of data that was coming out of the missile.

The last thing I need to talk about is the experiment involving the waterways experiment station. This was an example of planning for a test. Prior to OPSEC, a test was conducted which involved a given amount of a known explosive detonated a certain distance away from a model, and that model was a model of a BMD component. This test was conducted in the open and the report of the test results was initially unclassified, even though it gave very pertinent information. The levels of information generated during the test, and this had to do with over pressure, was essentially the same as the secret design goal. Of course, this report was quickly upgraded to SECRET. But the test itself was still open to direct observation. And virtually the same SECRET data could be derived based on that operation, which was out in the open.

Through our OPSEC program, several counter measures were identified. The planning for that effort included participation by the prime contractors, sub-contractors, project office, region representatives and others. This type of planning and coordination is necessary and is actually critical to the success of the OPSEC program.

There are some key OPSEC issues. How do you handle sensitive unclassified? If it's targeting information or intelligence indicators, and may require more protection than security awareness, we've been upgrading it to CONFIDENTIAL. We've established a committee, technology transfer termination working group, called a T-3 Committee. It's composed of government, industry and others to try and get a handle on what is reasonable to do regarding the sensitive unclassified, and the loss of critical technology.

There have been many discussions between government and industry as to the subject of monitoring OPSEC compliance at the contractors facility. The Defense Investigative Service feels that they should check compliance during their regular investigative service inspections. There's something good to be said for that. Currently, we are having this done by the 902nd personnel. This is because it involves them going back after they provided a threat briefing and helped them to prepare their OPSEC plan, checking to see how well they're following the plan. Also, if there were things that were missed.

Someone mention yesterday about the DOD directive. That's being staff read, still at the Army level, and will be published sometime very soon. Depending on what comes out, it should give us some good guidance as to what we need to do.

I think OPSEC is here to stay. It certainly filled a void in the BMD program.

This concludes my remarks on OPSEC.

**Lee Killen**
**Physics International Company**
**Martin and Stern Group**

I would like to discuss the subject of OPSEC at a little higher level than what we just dealt with.

What I'd like to do is discuss five aspects of the problem. First of all, I'd like to give you a little prospective. I'd like to discuss what's happened in the environment that might make OPSEC an

attractive vehicle to do business with. Next, a little bit about what OPSEC is. Everybody has their definitions, so I won't bore you with the definition. I'll give you an idea of the color that I paint OPSEC. Also, I'd like to provide a little bit of my personal philosophy on how to deal with OPSEC problems. Additionally, the unclassified sensitive information problem.

The basis for developing weapons systems is to provide us a competitive edge on the combat field. What I have here is an attempt to show you what happened since 1965, in terms of the available combat power that we have. It's a bit over simplified, but I think it provides the pressure of the correct image.

Back in 1965, we obviously were quite a bit ahead of the Soviet Union. They had a lot of people, but they were relatively unframed and their systems were relatively unsophisticated. We had this magic thing called "high technology" that gave us a competitive edge. In fact, forced multiplication remains to this day as a major cornerstone of our defense policy.

Over the ensuing 13 years to 18 years, a great deal has changed. The Soviet Union has continued to produce the same numbers as they had before, where as we have slowed down our processes. What has happened is they've introduced between 2 and 3 new or significantly improved weapon systems to every 1 that we've introduced. Even more alarming, they are introducing high technology into these weapons systems at a much greater pace than ever before.

The bottom line on this is that our forced multiplication cornerstone is being erroded very seriously. It's not just my personal opinion. I put the USA as a questionable equal so that I wouldn't get any babbles from anybody. My personal opinion is that we're far from equal, we're way behind and we're desperately playing catch up.

The information to support this prospective is in these two documents, Soviet and Military Power. They're produced by the Department of Defense. They're basically marketing tools by the Reagan Administration to get his budget passed, but they're excellent. They're well done and based on my intelligence background, and knowing what the figures really are, they're accurate. They cost $6.50 each, government printing. I think they need to be mandatory reading for everybody that's involved in systems development and RDT&E.

In case you weren't going to take my word for it, I've brought along a little bit of horsepower. President Reagan is of the same opinion as I am. There are 3 key elements in this quote, one is the word "restore" the next one is to "achieve parity." We are in fact behind by his opinion and it is going to have to be done by our own effort. The Soviets are a determined adversary. They are not going to let us catch up easily.

However, in view of the recent controversy over presidential quotes that we've been seeing in the newspaper, I've brought along extra help. The military prospective says the same thing. This quote by the Secretary of the Army also has two important factors in it. One is "the most serious threat" and the next is the "high imbalance." We're in fact behind.

How did this happen? We have our traditional security programs. They're protecting all of the classified information. In all of my efforts in the OPSEC program and in doing large scale surveys at five major tests centers, White Sands, Lackland Air Force Base, Patauxant Naval Air Test Center and one or two others, I seldom found a case where classified information wasn't being protected adequately. But this has happened. The Soviet Union has made these achievements despite these.

How could it happen? Well, in order to answer that question, we have to look into the environment within which systems development and RD&T takes place in our country. I've identified three fundamental aspects of this environment that have changed dramatically in the past 18 years.

What I have next is sort of a compara-contrast of the technology in the years. And I've looked at three aspects of information availability.

As we all know there's been literally an information explosion available to the general public from open sources or even from government. At the heart of the whole thing is, of course, the

computer and our electronic data processing capabilities.

These three aspects are inter-related. So when we talk about them, each one reinforces the other. There's a bit of a centerism that evolves from this. Together they are much more significant than each of them would be on an independent basis.

Basically in 1965, we were dealing with carbon copies. It was very expensive to make a lot of copies of information and documents, so very few were made. Distribution was limited on the practical problem based on reproduction. Now, information reproduction is cheap, relatively speaking. As it's become cheaper, the demand has increased dramatically to the point where now there's virtually unlimited copies of any kind of document that you would like to get, if you can get it. It's not going to cost you an arm and a leg. We have electronic distribution of these things so it's available in a lot more locations than it had been prior to this. We also have the enormous data bases that the modern computer capabilities allows us to deal with. We have things like the National Technical Information Service. We have Orpinant, which is a computer system set-up to facilitate the exchange of information. Under government policies, a number of things have happened. In 1965, there was little difficulty in classifying information. Now the emphasis is and has been on de-classification, open government, and letting the people know what we in government are doing. It's their money.

Things have come along such as the Freedom of Information Act, need I say more. As an ex-intelligence person, I personally believe that some clever Soviet agent drafted that document for us. That document has probably done more damage to the security of this nation than any other single vehicle.

In addition to that though, we have had some official government sponsored problems. Technology transfer appeared to be an open policy of the government in 1972 in order to improve relations with the Soviet Union and other Soviet bloc countries. The growing emphasis on de-classification and making information available.

A defense market place also provides an enormous amount of information that was not available back in 1965. In 1965, we had a relatively straight forward business environment. There was exchange of goods and services for money. The government made a contract. Now, the government is injecting competition at a level never dealt with before. We have shoot-offs, we're going to extraordinary measures to prove to the people in the country that they are in fact dealing on a competitive basis. Nobody is making any millions of dollars on that.

Sole source has become a four letter word in government. We also have the social issues involved. We have small businesses, disadvantaged businesses, minority businesses, and all of these things have gotten in the way and what they all do is increase the amount of information that's available to the general public.

The next element that has changed dramatically is the intelligence process itself. Computers have also revolutionized the intelligence process.

Intelligence collection is essentially gathering information. The computers significantly fit into that. The Soviet Union military, like our intelligence, gets the best that's available in the country. If there's a new computer developed, the military gets it first. Within the Soviet military, the intelligence community has first shot at all the most modern equipment. So it's being used about the same way as it is in our community.

The analysis capabilities of your typical intelligence analyst, in 1965, were somewhat limited. An intelligence analyst is only as good as his data base. It's only as good as the amount of information that he can correlate with new information by the people who are collecting for him. Now, we have virtually unlimited data base correlation capabilities. What this does is allows a centerism to take place here, wherein each piece of new information that's collected by the collectors gets compared against the data base. And so it permits a more complete exploitation of this new data. Conversely, when the new data is added to the data base, it updates the value of the information that's already resident in that data base. So we're getting it on both sides of the coin with this.

In management, in 1965, intelligence (the intelligence collection) was largely a series of people who were operating in a relatively un-coordinated fashion. They were given tasking and they were sent to collect what they were to collect, and they didn't talk to each other on a frequent basis. Even further than that, the managers of the collection agents didn't speak to each other a lot. Nowadays, it's correlated. We have again the computer data bases that allow somebody to go in and look and see what's available, find out who's available to collect the kinds of information that's needed, and it's done in a very orchestrated fashion. It's also a much more businesslike thing. The computerization of it has brought in things like return on investment, and allocation of assets. It's attempting to get the most bang for the bucks, so to speak, in the intelligence business. I'll speak about that later. I call it the rational mad concept and it's way of dealing with problems.

There's also been a dramatic shift in the targeting of foreign intelligence operatives. In 1965, they were basically looking at government for economic and political information and the military for military information. Now, the whole thing has become so inter-related and so complex because of the amounts of information available and the sources it's available from. We're finding that most of the spy cases that have been developed over the last couple of years have involved the industry rather than the military or government.

The objective is to get the information, get the raw data before it becomes subject to the government classification system. It's a lot cheaper for them to do it that way. Industry applies the protective measures that are paid for in the contract. Industry operates on a dollar basis. If the government doesn't pay them to protect the information, they really don't have the inclination to protect it for the most part.

The last item on this is aggressiveness. In 1965, we had the basic cloak and dagger operation. There were guys going about with capes and all that sort of thing, but that's changed now. They're becoming increasing bold and much more sophisticated than they've ever been. In recent years, they've found Soviet agents going through data bases. Using an entry into a data base that they had access to, they link up to another data base. It was a rather large spy scandal in Vienna, Austria, where they found a Soviet agent that was suspected of being in a west coast data base of a U.S. company.

Intelligence collection has always been an aggressive type thing and there's a little saying I've heard many times over that kind of illustrates that and it says "In God we trust, everybody else we monitor. If we knew God's radio frequencies, we'd monitor him too."

The last element that has changed dramatically since 1965 is the time factor. If you give an intelligence agent enough time, he's going to get the information he's after. Time is a very critical element in the protection of information, and is particularly so when we're dealing with unclassified information with which we can only apply a limited amount of protection. So the answer to the basic question of "Do we need OPSEC?" I believe we definitely need OPSEC. It's not a subject that should be in lieu of traditional security programs, rather it's one that should compliment the security programs that are already in existance. It's going to have to be a collected effort in order to work. Also, it's going to have to involve government, it's going to have to involve industry, and the last element of the RD&T community as I call it, academia, is going to have to get involved in this. It's going to cost money, the government's going to have to pay for it, somebody's going to have to pay for it, but I think a lot can be done without spending a lot of money.

Basically the adversary is getting his information. That's obvious from looking at the weapons systems that are being produced in the Soviet Union today. In many cases, you can track U.S. technology as we develop it, and they're two or three years behind us. Well, low and behold their airplanes look very much like our airplanes and their capabilities are very similar, except they build three times as many of them, or five times as many of them, as we do. Also, I believe that the traditional security programs have been doing their job. As I said earlier, I have seldom found the situation where there was obvious security errors of any magnitude whatsoever. We do, in fact, protect our classified information from outside exploitation.

I think the fundamental problem is that we cannot classify everything that needs to be classified. It costs a great deal of money to classify something and then protect it and it just can't be done. The expense is more than anyone can deal with.

How can OPSEC deal with this unclassified, but sensitive information issue. Well, I'd like to give you a couple of characterizations of what I think OPSEC is.

First of all, it's concern with the entire operation. The first portion of the acronym is operations. So OPSEC will vary dramatically from one operation to another. What's needed in one may not be needed in another.

Secondly, it looks at information of intelligence value. It's not concerned whether it's classified or unclassified. It's looking at it from the adversary view point, saying what kind of information is going to satisfy this guy's intelligence collection objectives. And very often, it's not what we classify. The idea is to place yourself in a perspective of the intelligence collector. Find out how he goes about doing his business. What kind of resources does he have available to him. What are the problems affiliated with that kind of a collection process. Intelligence collection is not an easy job. It is very complicated. It is very expensive.

I think another aspect of OPSEC that's very important is that it's systematic. It looks at the whole picture. It doesn't just look at the curve view under it's scope. For example, OPSEC has a limited view. It deals with communications only. Physical security deals with another aspect of it. In between these security programs there are little gaps that ultimately come up. OPSEC not only fills in those gaps and makes sure that they are small, but it also can give direction to the security program by telling them what it is they are doing and why they are doing it. It understands the intelligence process and translates it into policy guidance.

The final thing is it's concern with effectiveness. We've become a nation of M.B.A.'s, where return on investment is the God or our objective now a days, and it's a short run policy. We need to look down the road and see how good is it, or how effective or efficient is it. If we develop a very expensive weapons systems and deploy it and find out the Soviets have already developed a counter measure for it, we've achieved nothing. And it's happened.

How does OPSEC go about doing these things? Well, once you know what it is that you want to protect and what types of information, it's just a series of steps you can work through very much kin to the process that Dave Brown showed on his slides, his analysis process. You find out what the threat is first. And the threat needs to be tailored to the operation that your looking at. A threat is very dependent on both the nature and the environment in which it's going to take place. If you find that there isn't any threat, then there's no point in spending money to protect against it. It's a very pragmatic judgement process.

This has been mentioned a couple of times before, a threat is in fact dynamic, so you can take a canned threat statement and apply it to a half a dozen contracts that may be occurring over a long period of time. When a security classification guidance is put together for a project, it should be recognized that as that project evolves from an R&D in-house environment to a developmental test and evaluation, at some test center some place, not only do the vulnerabilities change, but the threat changes. They're doing different things so you have different vulnerabilities. Your going to have to rely on somebody at the test center to tell you what the threat is at that particular site. We do it now as we draft our classification guidance, it's boiler plate that never gets changed, nobody looks at it.

Next you find you match a threat with the kinds of information that that threat can't get out. You see what type of information is made available from it. This requires some feel for the intelligence business. Again, you have to know intelligence is collected in order to do this. Then you assess the value of that. Again, we're dealing with the intelligence value of the information. We're not looking at classified information or unclassified. We're saying what's the intelligence value of the data that I can get using these simulated or hypothetical foreign threat passes to collect on this operation. The information is relative to, and

we cannot deal with it on an independent basis. One bit of information by itself may be meaningless. If you put it aside, alongside another piece of information in a data base such as intelligence data base, it can become an entirely different thing. So you have to relate the issues back and forth to each other.

And the last one, I think the key word is prioritize. We don't have an unlimited amount of funds to deal with these problems. Particularly unclassified information. What that says to me is, we don't have to have 100% protection. We're dealing with unclassified information.

How do we resolve these problems? I mentioned several times that the resolution of them, in my opinion, requires some kind of insight into the intelligence collection process.

Well, these four factors have got to be present in order for an intelligence agent to collect the information. If he's not aware that you're doing something, than he's certainly isn't going to task an asset to collect against it. If he doesn't think what you're doing is of any value to him, he'll certainly not be motivated to task that same asset. Again, he's got a return on investment problem. The rational man concept. This collection manager is going to task his people to produce the information that's going to get him the greatest benefit for their expediture. There's also the element of risk involved too, and that's taken into consideration. If he doesn't have the capability to do it, to collect against you, your operating in a frequency range that involves new technology and you know the Soviet Union doesn't have that technology, then again he can't collect. Not from that aspect of it anyway.

The following one, of course, is opportunity. The classic in this is over head satellites. Exploitation of photo satellites. If the day is cloudy, and you have complete cloud cover, that satellite cannot exploit what you're doing on the ground. So the ideal process is to reduce each one of these factors a little bit in your deliberation over what measures to put in place to deal with the subject. Make an incremental improvement in each one of these things. Make him a little less aware of what's going on, a little less motivated to think that it's of value to him. Do it in a way in which he doesn't have the capability to exploit it. Take advantage of opportunity, such as cloud cover.

This is sort of like a chain. If you can break the chain on any one of these things, theoretically, you can't have exploitation. Now I realize that this is a theoretical model. Again, it breaks down somewhat in practical use, but it's very useful in trying to deal with these problems. It gives you a starting point.

Over the years of doing these surveys, and once we got the survey, we identified the problems and prioritized the problems for the test range commander. Then he turned to us very often and said, "What do I do about it?" Well, that was the last part of the job and in many cases the most difficult part.

I've developed a little bit of my personal philosophy along the way that has evolved from a lot of sweat over a lot of late evenings at these tests centers. The basic assumption that I have gone under is everything cannot be classified. We just can't do it. Everything that ought to be, can't be.

The number one rule here is so important. It can't be overemphasized. U.S. security managers know that if you go up to your engineers and discuss a security problem and if you discuss it in a way that is going to effectively shut him down, he's going to shake your hand, say thank you and is going to do it anyway. You've achieved very little. So the basic issue is that there's a little thing called Wyler's Law. It's sort of like Parkinson's Law and a couple of others. It says that "Nothing is impossible for the individual who doesn't have to do it." And too often, that's been the result. When you go to a test center commander or project manager, and effectively shut him down, again you've done nothing.

The next one is, break those problems down. Let's do it on an incremental basis. We're dealing basically with an unclassified subject matter. The classified information, as I said, is adequately protected in it's entirity. There may be some minor disturbances here and there, but basically it's taken care of.

This is the big one. If you break it down into it's components, look at the big problem and say

what contributes to that problem. What are the elements that are involved in that problem? Then look at those elements and say what can I do about each one of these elements. Can I improve each one of them incrementally? Once you've gone through that process, reassemble the problem. Take a look at it and see if it's still as serious a problem as it was when you first looked at it. Very often, I've found the problem is reduced in magnitude and when you go back to your prioritization of the problems, it falls way down below. And you go on to the next higher priority problem to deal with. And of course, approach it in the same manner.

Another aspect is that, since we're dealing with unclassified information, a 100% protection isn't necessary. We don't have to guarantee it to the nth degree. The 80% — 20% management principle says that you can solve 80% of your problems with 20% of your assets. It's a proven management principle taught in all the M.B.A. schools around the country.

The other side of that is that it will take the *remaining 80% of your assests* to solve those remaining 20% of your problems. So my philosophy is, let's deal with what we can deal with first. Solve the easy problems. Don't tackle the tough one. To often people jump right into the sensitive, but unclassified thing, and treat it in it's entirety on the largest scale. They'll look and say, what good is it for me to start making these efforts or these initiatives, in my location, when I can go to the congressional record and read all this stuff. And it's free and the Soviets subscribe to it.

Well, you've got to start somewhere and as you'll hear later on from another speaker, there's a lot of emphasis on government to deal with it at that level.

Vulnerabilities are inter-related, which is another aspect. If you have an agent targeting your operation or organization, and if you change the amount of information available to him, his inclination is going to be to take a look and see what he can get from other places. So what was not being exploited prior to the changes that you made and the improvements, may in fact become exploited after you make them.

The final thing is that some problems can't be resolved. You just can't deal with them. It costs too much money. You'll have too much of a negative impact on the operation to be acceptable. It'll cost too much. It'll take too much time. It'll delay the operation. My feeling is that's fine. If you've gone through the analysis process and this is your bottom line answer, at least you know you have a problem. You've appraised the individuals involved of the problem. And they are aware that they have this vulnerability. Now, perhaps at some point in time, as I said, everything is dynamic in time. It may be feasible to solve that problem, but at least the problem is brought out into the open, and that's vitally important. Just to know what your problems are.

My last is the type of a program that'll do these things. These bullets here are oriented basically towards a test center, a large project, or a defense contracting firm. Any of the organizations could implement these types of things. They are looking at it from the top down. What I'm saying is I have never met a project manager or a test center commander that did not want everything he did to go unexploited by the foreign intelligence. But we didn't want to feel that the weapons systems that was completely or at least partially compromised when it went into the field. But their basic problem is that they're not intelligence people, they're counter intelligence people, they don't know how the intelligence business takes place. They are not aware of the vulnerabilities of various places they go to, because we have boiler plated classification guidance.

I think it takes policy guidance from the top levels. Goals and objectives need to be established. What are we trying to achieve in this area? Minimum standards at test centers, they have minimum standards for safety. Why can't we have minimum standards for security? Or for the protection of all information? Those things need to be tailored to the particular organization, operation or project that's involved. It can't be, again it can't be legislated by government. There needs to be comprehensives. Somebody has got to be put in charge of everything that goes on in that project, and that test center or in that company. And the person has to have access to management. He should be the person who surfaces the

combined problems of all the traditional security fields and brings it to managements attention that advises them of the situation. I think that education and awareness can go a long way to dealing with most of these problems. As I said, people care and they don't want these things to happen, they're just completely overwhelmed by the magnitude of the problem.

Another aspect that's missing, almost completely from this area, is active support of the intelligence community. The intelligence community, both at the national and military level, devote almost all of their assets to active duty, to the ships that get underway, to the planes that fly and the tanks that move. They don't actually think of RDT&E as an operation. They think of it as something that goes on in industry and we don't have to worry about that. But it is very much an operation. About the only interface that ever takes place in this is from the scientific and technical liaison officer. And he's not looking at it from the right prospective.

I think basically the impediments right now are organizational and operational. I think that there are plenty of people in the traditional security programs, and they're good people, that given a bit of guidance and given a little bit of support from management, can deal with much of the issue. We can go a long way before we have to hire the first new guy. I guess that the last issue would be, "What does this have to do with industry." We're talking about weapon systems, we're talking about ships and airplanes. The government does not build ships and airplanes. The government basically does not develop and push forward the barriers of technology, it's done by industry. The government pays for a large portion of it, and in many cases, directs it, but still it happens in industry. And right now we have a very serious problem. Thank you.

**Richard Cary**
**Vought Corporation**

As a classification management specialist, one of the reasons I wanted to talk to this group is that the one thing we have to do is make sure that we realize that particular technique that we're talking about is nothing new from the standpoint of common sense approach. I've seen OPSEC pushed from the military standpoint nationally. It was a success. I've seen the OPSEC attempt to be put into the international community, the NATO community, and it failed miserably. A communication job is the reason it failed over there. OPSEC is a part of common sense. It was just as obvious to many of the security professionals in Europe, that OPSEC is the way to go, as it is in the American community. The unfortunate part is the operators didn't buy it, because the operators didn't see where they had to get involved in it. This is a security problem and we didn't sell the project idea of OPSEC. We'll start off saying that it is not a new approach, and we have to accept it. It's as old as common sense.

Second, there are several things that you have to have if you're going to have an OPSEC application.

The first thing you've got to have is the need for that kind of a security application to the problem that you have. That is the reason that we have BMD, whose sort of a pioneer in the field, involved with OPSEC, and they're very concerned with it. You can see through the years they've been in it. It's dynamic. The things that they build lend themselves to the OPSEC approach. Many of our major commands are dealing in studies and research and things of that nature. It does not lend itself to that kind of approach. Attempting to force this into that kind of a security program could be a very serious mistake.

With respect to vulnerability (the threat data), I've been very encouraged today. When Clark mentioned he had this group together, that removed one of the primary obstacles that I've always seen in OPSEC in industry. We do not have the access to the kind of data you can get in government because they have the clearances, and the contacts. You can call up and can go into the little green room, and you can sit and they give you a real good run on the threat. We in industry have never had this kind of data available to us and generic threat data is not sufficient to do real OPSEC. The vulnerability data has to be provided by operators or security specialists, or security professionals and I consider myself one. If we don't know what they do, we cannot possibly do the kind of job OPSEC requires to be done in order to come up with vulnerabilities. It's

primarily humint espionage. There are many more threats in many activities in this country that we have to be aware of.

The other thing that the OPSEC community has to realize is that we are not going to have the program approach that you heard from both BMD and this speaker. We heard from Tom O'Brien and also from contacts, that OPSEC in the industrial community is going to be applied on a project basis. We must realize that we're not talking about a program that is a continuing thing within an organization where you have people assigned to do OPSEC. It's going to be formed at the time the contract is provided. Contrary to opinion, private industrial security is not paid for. The industrial security program is not a paid program. This program will be, according to what Tom O'Brien said, on a pay basis. With this in mind, the comments that I'm going to make are within those perimeters.

In reply to the question of where is OPSEC up to date? The answer is at the point of no return, sitting at the same fork of the same road the military traveled, saying "Good grief, they really mean for us to take this trip. Now, what direction do we go?" If OPSEC's current appeal is to be maintained, and it's full potential to be realized, we have to make the right choice in direction. Time will not permit for me to discuss the program approach that I'm completely in favor of. I'm going to address the currently accepted narrow approach of applying OPSEC concepts to selected projects at the RFQ contractual base.

The OPSEC requirement search contract says that you can take one of those two directions. First, one part of the road leads toward OPSEC becoming a mandatory pre-conceived security requirement that's routinely applied to all sensitive, but classified government contracts. The requirement would be based on a generic threat to protect generic Essential Elements of Friendly Information (EEFI). This protection would be achieved by establishing a required set of counter measures that would be generally applicable to protecting classified information and the counter measure to be outlined in the standardized OPSEC plan that would be subject to a check list inspection. That is what it can end up being if you stamp it with the OPSEC. If we do that, it's going to become a routine thing. Somebody's going to form a template and you're going to fill a space out on the thing and OPSEC will go down the drain in industry.

The other fork of the road leads towards a systematic approach. It's designed to determine if a protective measure that exceeds the existing security program must be applied. The planning sequence would begin without any pre-conceived notion that our formal OPSEC plan is going to result. The planning will be based on what I call legitimate EEFI, and I'll discuss that later. This EEFI ought to be provided by the contracts security office. The vulnerabilities would be analyzed in context with the local threat environment and if deemed advisable would be incorporated into an existing security program where possible. The remaining safeguard would be subject to a risk analysis procedure. When it is finally determined that a formal OPSEC plan would be called for, it would be narrowly focused on those problem areas that we cannot solve by locking it up, classifying it or doing something else with it. My examination of current OPSEC guidance, and my review of a few draft OPSEC plans, indicates that we might be proceeding down the wrong road.

Now, I'll address only three short comments I've noticed.

One problem area seems to be the definition of EEFI. That means essential elements of friendly information. This term is being used interchangeably with vulnerabilities and hostile EEI. In hostile information they need to do their job. For example, a list of scheduled field tests of a system would create a vulnerability for us. Just having that list as to when we're going to schedule these field tests is a vulnerability. We have to protect it. The enemy needs to get access to this. That becomes his Essential Elements of Information (EEI). But neither of these situations would cause this particular list to be referred to as EEFI. I've seen some plans where this kind of information is listed as EEFI. EEFI should refer only to the basic critical aspects of a project that must be protected at all costs. If we cannot identify something that's that important we should go into this very detailed process to figure out some way of protecting it. We should check on whether you need an OPSEC plan for that particular project. In

this vein, I can't visualize a legitimate list of EEFI that would not be classified to the highest level of the project. The EEFI, if it's something that's that important, should be classified or else you couldn't tell me what it is without me already having blown your OPSEC objective.

Another problem area seems to be the listing of several types of countermeasures within formal OPSEC plans. Not during the planning phase when you're just figuring out what we have to do, but it's the final product I'm speaking of. For instance, the decision to classify certain sensitive information is a matter for existing classification guides. It should not go into an OPSEC plan. There's no such thing as OPSEC confidential. The placing of prescribed countermeasures in the proper security program will greatly reduce the size and the scope of the formal OPSEC plan. This is essential to gain their meaningful participation of the operational aspects of a project. The more you have to talk with the operators, the scientists the engineers and those kinds of people, the more you have to talk with them about the security threat. The more they get turned off, the more chance is that OPSEC is going to fall flat on its face.

The final problem seems to be the application that every OPSEC planning requirement must result in producing a formal OPSEC plan. The requirement for the nature of an OPSEC plan should be based on the mutual needs agreed to by all parties concerned. The government, the contractor, the operational people and the security professional. I reiterate, based on what I've said, the current acceptance of the OPSEC concept by the non-security elements in the industry is due to the fact that it is a common sense approach. Most people, once they understand what this is all about, agree. We have to do something because what we've been doing in the past hasn't worked. This is nothing but using our brains to try to address a problem that exists. Now if OPSEC becomes just another non-sensible, mandatory security program that's routinely applied to every classified contract you get, that appeal is going to be lost. Soon as you mention the name, peoples' fingers go in the air and don't say that it is a government requirement that they have to go through this planning because we won't let you have the contract. Engineers, scientists and people who do meaningful work will not allow you to waste their time if you can't convince them it's worth that time. They'll quit a company before they'll sit down and go through a lot of mish mash with you.

Now the last. If the EEFI listed does not clearly meet the criteria of EEFI, it's essential that we protect this portion of information. Not the fact that we're building a tank. That can't be protected, Not the fact that the tank is going to track suspension or that the tank is going to have a main armourment. That's not essential. It might be just the one fact, that the tank is going to have spaced armour and this spaced armour is of unique design that is going to give this tank a great advantage on the battlefield over the other guys tanks. If he knows that at the time we started building our tank, he's going to get a counter measure. So when you bring that on the battlefield, he'll either have something that will penetrate it, or he will devise something that will lessen its effect. That one thing, EEFI, is based armour. All the other classified things are sensitive, but not EEFI.

Now, if the OPSEC countermeasures become cluttered with requirements that can be left with us specialists, classification things that we can put into safes and so forth, we have a security program that will handle classified documents. We don't have to bother operators with this sort of thing. If we can get the requirements delegated to the security department, then we can concentrate on giving the operation security that cannot be addressed by existing programs, OPSEC will succeed. If we do not, the security departments will end up with the security job as a unilateral compliance requirement for the contract and if that occurs, these trips that we were going to go on will end up right back where we started from.

That's basically what my concerns are from an industrial standpoint. That we don't turn them off, before we turn them on.

**Paul Blatch**
**Naval Weapons Center**

We are an organization that is essentially ADHOC at this juncture. We are looking for sanction from our parent organization NAVMAT. It involves the

core, if you will, of the eleven Naval Research Development Test and Evaluation (RDT&E) capability, spread around the country. We call ourselves the RDT&E facilities committee and operations security. We are looking at vulnerability and threat and possible solutions of our problems in the RDT&E community.

All the other things you've heard about and read about OPSEC, probably to one extent or another are true. We view it as this: That OPSEC is an umbrella that coordinates and integrates the other traditional security measures. This includes COMSEC, Physical Security, ADP Security etc. . . . (See figure 1) All of those areas are fairly well documented. You have professionals working in that arena. You have the kind of measures they are now taking that are very mature, but they all have problems as you all know, that work in those fields. Security managers say that they don't have enough personnel or that their responsibility is fractured, and they can't get the documentation that they need from time to time. They cannot do their jobs as well as they would like to. OPSEC hopefully, in that arena as well as others, will provide some kind of liaison to upper management, provide some kind of cohesive integrated program that if you have vulnerability in this area and not in this area, it is not going to do any good to continue the strong emphasis in this area if there's going to be a loss on this side. We'd like to look at it from a wholistic approach, if you will, that we are going to provide some methodology whereby from an OPSEC point of view and intelligence point of view, looking at ourselves as an adversary would find those gaps as we mentioned, and find the ways that we are vulnerable to exploitation and get rid of them. (See figure 2)

The objectives of the committee are six. Basically, what we want to do is institute the capability of OPSEC within each of the RDT&E facilities. With the position of OPSEC officer, that officer will be on a high level, with direct access to the technical director and/or the commanding officer for the purpose of addressing OPSEC on a command level, working with project managers, the program managers, the security people, intelligence community, any and all people that are necessary to make this thing work. (See figure 3)

The whole deal is that we consider it most critical. This is just a partial list and it's just meant to be representive, to telemetry, voice, video, microwave, data, telephone, all the things which deal with communications. However, there are things that we cannot address because of dollars and a few other things, including technology. I'm only going to take one of those. Video is coming, voice we know about, telemetry is still having a problem, in fact, numerous problems. Microwave is exploitable. I think that's been shown by the OPSEC surveys. We know the problems in ADP security, they're not getting better, in some ways they're getting worse.

One technology, the telephone, sits on your desk and it sits on my desk, it sits on every desk. And if you had a $135.00 line actuator and you know what lines are going into any telephone, on the table is a microphone. When someone taps into that they hear everything that goes on in your office. We all have that kind of problem. In the ADP area, we're talking about documentation 5239.1, which is the ADP security managers guide. It is being re-looked at. Some people have become unhappy with it because of conflicts. That document needs to be improved. We need to improve the way that we're structuring data bases. We need to improve the way that we're looking at what's classified, what is not classified, especially from the area of sensitivity. What we're looking at now is that there have been several documents, DOD, as well as Navy, that says you will protect all information dealing with weapons development. We're not doing that very well right now. Point of fact, the unclassified, because of the problem you cannot classify everything, therefore you make a determination on which should be and which should not be. Those things that are not, in the aggregate, do compromise certain critical elements that affect the system development process. We need to take another hard look at that.

The public affairs officer releases public releases to the media and to other organizations. He takes what he needs from the project manager. The project managers are not aware of the criticality of their particular piece in a systems development. They will say sure, let's talk about this. We also have the publish and perish syndrome. They want attention for their project, understandably, and they give those kinds of high impact state-

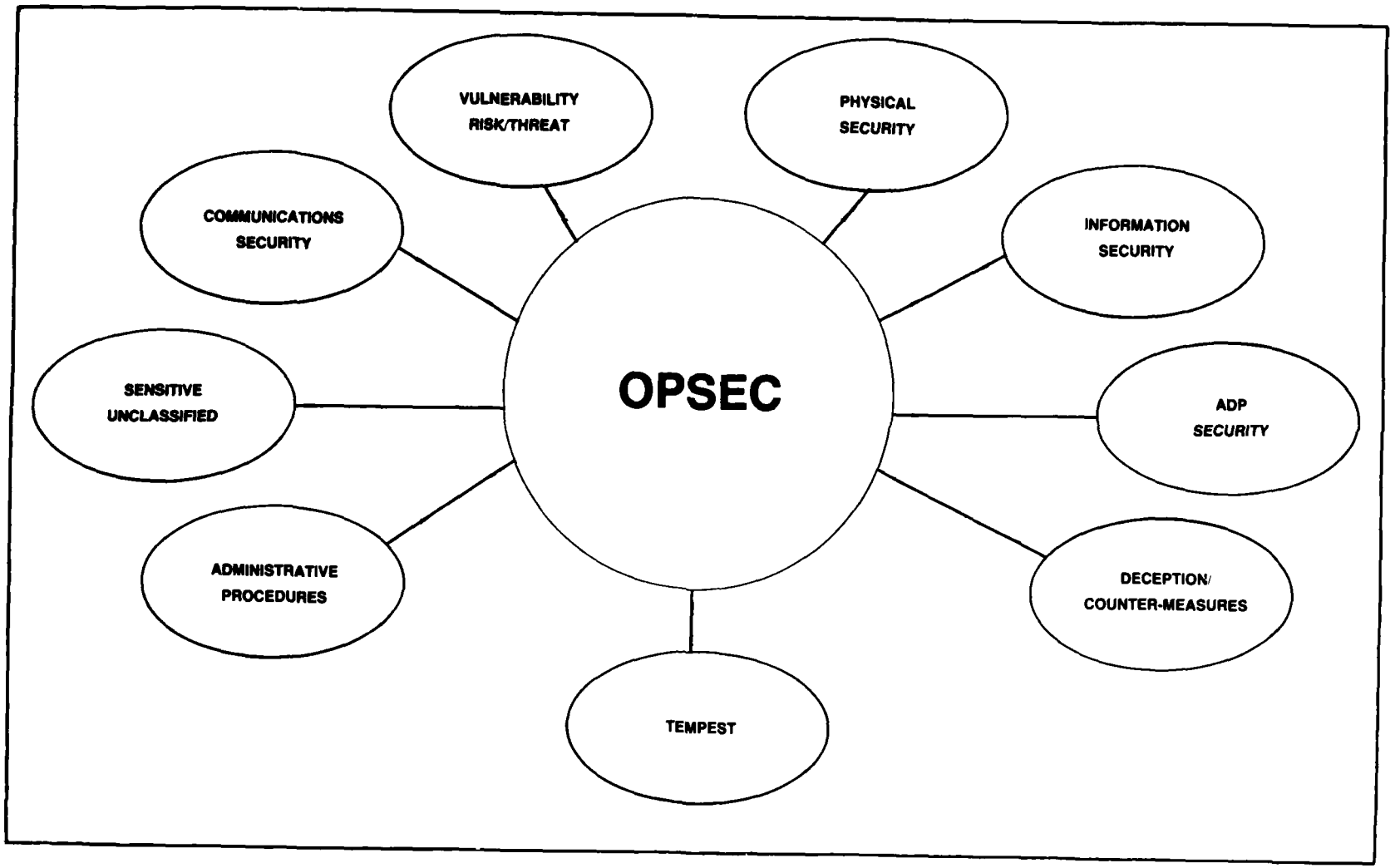

VULNERABILITY
RISK/THREAT
PHYSICAL
SECURITY
COMMUNICATIONS
SECURITY
INFORMATION
SECURITY
OPSEC
SENSITIVE
UNCLASSIFIED
ADP
SECURITY
ADMINISTRATIVE
PROCEDURES
DECEPTION/
COUNTER-MEASURES
TEMPEST

FIGURE 1

# OBJECTIVES

1. Support OPSEC principles & functions within the DON RDT&E Community.
2. Provide RDT&E facilities with OPSEC focus and a common set of concerns to address immediate OPSEC priorities.
3. Develop OPSEC support capability within each RDT&E facility to support OPSEC officer in performance of duties.
4. Share openly & freely any & all information relevant to OPSEC function to further understanding of principal issues & concerns.
5. Perform studies & analyses and make recommendations, through chain of command, to organizations having effect on OPSEC program(s) so that they may be advised of RDT&E posture & status with regard to OPSEC matters.
6. Provide an information repository and an OPSEC corporate memory.

FIGURE 2

# VULNERABILITIES

- **Communications**

  telemetry microwave

  voice data

  video telephone

- ADP
- Unclassified Sensitive
- PAO/coordination
- Technology
- Physical

FIGURE 3

**". . . The United States R&D establishment is viewed by the Soviets as a mother lode of important and frequently openly available (Science and Technology) information. In fact, they tap into it so frequently that one must wonder if they regard U.S. R&D as their own national asset. They have enjoyed great success in this endeavor with minimal effort, primarily because, as a nation, we lack the awareness of what they are about."**

**DR. JACK VERONA**

**Assistant Director of Scientific Intelligence Defense Intelligence Agency from "Transfer of United States High Technology to the Soviet Union Block Nations"**

**Report of the Committee on Governmental Affairs—United States Senate, 15 November 1982**

**FIGURE 4**

ments that go out the door. This may not mean anything by itself, but in the aggregate, from all the other statements that are made, they do mean something. We need to look at that function also.

Technology. We can't use fiberoptics now, because they're a way from being able to have a system that will handle fiberoptics. We also cannot encript above millions of bits per second on a telemetry system. There's a number of things we cannot do. We cannot exploit the technology because the beaurocratic system moves slowly in some ways, and in other areas it's just because we're not looking at those kinds of things. That's not to criticize any of the congress and authority. It's the just the facts of life. But we need to do something about that on a systematic basis.

Physical security. Physical security is a thing which we absolutely need. It's a first line of defense, but is often seen as the only defense or the major defense, and that is not where we're at today. Physical security has it's place but it is not going to keep people any longer out of ADP systems, it's not going to keep people out of your office automation system, it is not going to lend itself to the exploitation of information in the open source literature. Those things are beyond physical security. It is something they have to address.

Threat environment. There are reports that specifically target RDT&E facilities. Now, as has been mentioned before and as argued also, it makes absolutely no sense to field weapons systems that are going to be compromised 5 years before they go into the field. If it's too long a lead time, the countermeasures are developed and effectiveness of the weapon goes down the drain. You're talking about expenditures in the hundreds of millions of dollars for a non-effective product, or marginly effective product. That just doesn't make sense to us. (See figure 4)

A quote from Dr. Verona essentially says that we are giving away far, far too much and we're doing it on a consistent basis. Collection or hostile intelligence is not a major problem for the hostile intelligent agent. It is simply a matter of going to the National Technical Information Service in Springfield, Virginia. As they have done in the past, it used to be that the Russian van would drive up to the back door and get everything that was published that week. We found out about that, so they don't do that anymore. That was fine. The following week, the Czechoslovakian van backed up. So we're not making a lot of headway in that area also. There are numerous cases of compromise. The problem perhaps is that most of this stuff comes from open source literature. We have lost, just in recent times, the F-15 data radar systems, air to air missile, and surface to air missiles, and it goes on, and on. Now we have got to stop those kinds of things. We're spending many millions of dollars on the development of these systems. And they are not going to be what we want them to be. We're not

surprised by this anymore. We've just seen too many instances of it. The Soviet equipment looks just like the U.S. equipment. It's no accident. Many of these are blueprints of open source literature. They have easy access to it. It saves them a lot of time and effort. Essentially, what we're saying is that in terms of focus, sensitivity, common sense, awareness, we are our own worst enemy. In your field, classification management, you have a fairly strict doctrine, you have your interior problems, but by the same token, we're also talking about things that do not happen normally in the industrial relationship or in DOD infrastructure where we have the point of view that we can indeed accomplish a good preventative measure to losing these kinds of weapons and these critical data.

So we're in fact our own worst enemy. We let too much go out the door and we don't seem to be that concerned about it.

Focal points. We want to be able to support the command and as importantly, we want the command to support us. As I mentioned earlier, the various commanders have come up through the ranks. They have dealt with these things on a daily basis for 20 and 30 years, but they have priority problems. In the Navy, we have a high priority on drug related problems. So a lot of our staff and a lot of our resources go to that, not to the protection of the weapons system. We think that needs to be changed a little bit. We need command support to institute OPSEC and once that is instituted, then we can support command in the way that we think is proper. The 80%-20% measurement principle that we mentioned earlier is a correct measure, or at least in the ballpark. With a stroke of a pen you are not spending any resources or money, but you are saying you'll be doing things a little bit differently. You let the project manager make the determination on what they consider critical and non-critical and abide by that. You provide, in the area of physical security, an open base close to a semi-open base. Things that can be affected using minimum resources and minimum management attention can take care of some problems that are existing that does lower your vulnerability.

Contractors. There's really two problems in this area. Neither one of them are the contractors fault, it's the DOD's fault in my opinion and the opinion of the committee also. On one hand we have contractors who, once the officers are cleared, issue at their discretion company confidential clearances. Those people are not checked by DISCO for perhaps a year and half or perhaps longer, I do not know the recent figures on that. But they have access to sensitive areas. We don't know who they are. We don't know where they're from. We assume that it's a good guy relationship, but that assumption has not always proved true.

The other problem with contractual areas is that if DOD spends a lot of money, a lot of resources, a lot of attention, people like ourselves here on the panel and people like yourselves in the audience, do get into an OPSEC program. We do it well, tighten up DOD, and make it look like it should. As I think it was mentioned earlier, most of the defense contracts that result in weapons systems, development, or other systems for that matter, are done by industry. It makes a difference whether it goes from industry or from DOD. Both have to be conversant with each other.

Standardization. We're really looking at standardization from a point of view that if we do one thing at the Naval Weapons Center and its done differently at the Naval Ocean System Center in San Diego, there exists a gap. If we don't have a commonality, a standardization if you will, their function and focus may be different than ours. We lose things. We want to have a little bit of standardization so we're all talking the same language.

We're talking about an integrated factor that does not exist now. Certainly security professionals talk to each other, but their point of view is different, their organizations are different, their affiliations are different, the way that they handle business from one juncture to another is different. Something needs to integrate and coordinate those functions so they all work to peak maximum. That does not mean that they are aligned with authority over those organizations, merely an advisory to the command and to the individual organizations and a focal point.

There is a difference between the way range and laboratories handle their business. A range is where you fly the missiles and the aircraft and

shoot the tanks off and everything else. They have a geographical difference. The laboratory is more inside offices, and lab facilities. They do treat things a little bit differently. I think the range is marginly sharper than the laboratory, and brings together the requirements of other activities. There is a problem in that area, but it is not a major one.

Army, Air Force, and Navy exchanges and uses each other's facilities from time to time. There are over flights of various systems. They need to talk a little bit more and figure out what it is that they need to do as a tri-service or a group activity to make sure that we're not missing anything.

Project managers are the nucleus. They are performers. They are the ones who are most aware of their own projects. They should have the judgment on what is sensitive and what is not sensitive. They need to be participants. In the past we've seen that there are really two things that happened. One is that the scientist and engineer has got to get his program in on-time, on budget and it's got to work. Anything that gets in the way of that is advesarial. Security is usually seen as advesarial. We need to change that attitude and change that perspective and the way that we do business a little bit.

The technical community. We're talking about seminars, like this, that exchange information in open form, that publish papers. We need a little more sensitivity, a little more awareness of what we're about, of what other people are about, and especially the hostile intelligence collector to curtail that kind of soft leakage.

The third thing, information resources. We're looking at the aggregate body of data more and more. Dense repositories make significantly sensitive information easily obtainable. I don't think there's a technical director or commanding officer anywhere in the United States, Army, Navy or Air Force that you could not take into a hotel room in Des Moines and get 80% of what's on his data banks. It's been done before. In a couple of OPSEC surveys and in other instances. It's just a fact of life. We need to do something about that. That's wrong.

Dollars. We're talking about billions. Hundreds of millions multiplied into billions that we lose in terms of advantage, the costs that we have to bear and in terms of the weapons systems development. If we could elongate the procurement cycle of the Russian's by a year, that means a year we don't have to do another aircraft, another this, another that. We are going to save hundreds of millions of dollars on each individual weapons system development. In the 1967 to 1969 time frame when we fielded an aircraft it was five years before the Russian's had a counter. The time frame has been drastically reduced. Something is wrong. They're getting our information.

Iteration versus maintenance of security measures, everytime a task comes down into a RDT&E environment, we have to do certain things. The security plans have come down from the tasking organization and say do this, that and the other. We go and we do that. If we had the things set once, because the tasks are not that difficult, the telemetry is always telemetry, the data is always on data screen. If we set it right once, then it becomes maintenance. We don't have to spend those resources each time.

The critical loss for R&D data, I think that's a little self-explanatory. We are talking about, basically, those kinds of things that are critical elements to our weapons systems development. Whether it's particle, high laser or whatever it happens to be, we need to make sure that that doesn't go out the door because it means that we have to turn around and do it again next year. We have to go through Congress, we have to get appropriations, we have to have management resources, it does not make sense. If we can curtail the loss of RDT&E data for that matter, we are way ahead of the game. And we need to do that.

The last is a quote from Dr. Jack Verona, as referred to before (see figure 4).He says essentially that, they come in, they use our resources, they use R&D data. We have things now, if you have physical security on a R&D arrangement, you say you're going to get pass words to protect the data. I don't know of any instance which with the frequency with which pass words are changed that people don't keep a record in their pencil box, or the underside of their terminal or their telephone of that password. The char force or anybody else can come in and get that number,

and he's off with it. He's gone. He's going to get into your data banks. That's a simple arrangement. There are others almost as simple. In the OPSEC surveys, if you have a chance to read those documents, you will find other methodologies. It is very simple. They do exactly what Dr. Verona says.

That's basically what we're looking at in the Navy. The other half, the second half, if you're following this at all, and I should mention that at the on-set we are looking at least from the committee point of view today, is an immature look. It's a first cut, as to what we think an industrial security development program in OPSEC should look like.

Why OPSEC? You've heard various people mention this. Simple patriotism. It means that we do our job. Do it right and become more aware. Take that extra step, that extra effort. Develop in ourselves a consciousness and sensitivity to what it is or about, not just our own job. And that doesn't mean become snoops or harder workers than you already are. Just simply be aware. If you see an instance, if there's something you can do. If somebody says hey OPSEC or not? Give the benefit of the doubt, say yeah, why not. Take a look into it. Research. Whatever it may be, it's important, it is coming. I think it's going to be effective. Perhaps, the most effective method that we've come up with in this generation of taking care of certain problems. Simple patriotism.

Strategic and tactical realities. You heard Elmer talk about the BMD activity. It's real. If we do not have a strategic superiority in the weapons system activity, we are vulnerable. That vulnerable ability may translate into a first strike. That first strike means we all wake up to a large orange glow in the sky. We also face the same kind of thing. It could become a Cuban missile crisis in reverse if we simply do not have the advantage. And that's what we need to gain.

Cost savings and avoidance. I think over time if we can get tightly coordinated with the OPSEC function, both on the industry side as well as the DOD side, we're going to see a lot of cost savings. We will not do that 11 month iteration. If we can stretch it out to one year, we're talking about billions of dollars. At least hundreds of millions on major weapons systems and billions in the aggregate. That money then can go perhaps into orphan projects or what I'm calling open projects. Those things that have a lot of merit, that'll be interesting to look at, that we really don't know what that is, but they just simply don't have the priority to get funding.

OPSEC, in the opinion of the committee, is perhaps the most effective for the least cost security measure that we've seen, again, in the last 20 years. This subject has come and failed two or three times. In the early 1970's, in 1977, and now it's coming up again. I feel if we do not do it again, we're probably going to lose it. But I will re-evaluate, or at least second the motion that Dick mentioned. I think it's here to stay this time, but what it actually looks like at the end is what we're concerned about. If it's an administrative solution, or if it is a solution based on budget it is not going to be the right solution. Hence, our commitee, and I think other people working in other services at an LSD level, want to inject the reality of operational level people into it. That's why we're going through these kinds of forms and soliciting input also.

RDT&E and OPSEC needs three things. It needs coverage of critical data elements from the project initiation until it's field employment. If someone, for instance, in NAVAIR, says I think this would be a good idea. From the time he starts putting things down on paper or talking to individuals, that needs to be covered. Those critical elements need to be covered in that particular lab assistant development activity, whether it's a fuse for a missile, or whether it's a aircraft, whatever it happens to be, he needs to take those measures right now, before it goes anywhere. If it comes down into to a RDT&E, DOD function, they do whatever they're going to do with it. It goes out for manufacture processing, whatever it happens in the industry, or if industry is developing the systems itself, it needs to go right along with it. Until it gets into the fleet where they have their own measures, or into any operational activity, that needs to be covered. And we're talking about, as we mentioned earlier, it used to be four to six years. We could field the major weapons system. Now it's taking 10 to 12 years and beyond. That's not good. So if we do not cover those things along the way, it's going to be compromised.

Specialized product and procedures to enhance security, especially in the industrial complex. We're looking at things from acadamia, from the Defense Advanced Research Projects Agency, from industry, from a number of sources that OPSEC, I think, once you start practicing it, things will start to pop. We don't have X. We can't use the data encryption standards for national classified information, perhaps we need something else. Perhaps there are methodologies or products that just as a bi-product NASA used to do. They would do something for the astronauts for the space program, and it would pop up with a whole different kind of application. I think the same thing will happen in OPSEC. Once you get that view point and work under that umbrella, there are probably going to be opportunities to develop new applications for old things or develop new things for new applications.

Integrating and coordinating a working relationship. Absolutely essential. At Naval Weapons Center, we have well over 600 people from three or four corporations that do a lot of our facilities activity. They do our ADP systems, they are there, they are an integral part, and they are cleared. We have a working relationship over contractual lifes that put us in the arena of both contract management, as well as a side by side working relationship. That needs to be strengthed also, from the point of view of how we effect our contractual relationships. Whether they are a ADHOC measure that security has put into, whether it's put into right up front, or whether we're looking at performance of certain functions that are better left to certain individuals and others. Those kinds of things need to be looked at.

In your arena, in the industrial arena, you have the same kinds of concerns we have. You have the same sense of unclassified documentation, the same as was mentioned earlier, communications security problems. The information security, ADP, etc. There is a slight difference in the fact that you're usually off-site. If you have a facility clearance, you do certain things in certain manners. In classification management, you do it in a certain manner. But the OPSEC can do the same thing for you in an industrial base as it does for us in DOD. It is a partnership that we can then work across. Also it can be turned inward. And you can apply that to your own organization, and I'll address that more a little bit later. An industrial OPSEC does not necessarily need to be just for DOD applications. It can protect your own information. If you have proprietary information, or a new design, or a patent, and if you find you're losing any of that, or if that's a problem with you, try a little OPSEC. It may help you as well in that arena as in the other arena.

Specific mutual support examples. I present this only because things are happening that you need to be aware of, that you need to be proactive about, that you need to be informed about. What is the Air Force Westinghouse pact? That is essentially the Air Force Systems Command, Electronic Systems Division, who has essentially devised and implemented with Westinghouse a pact that says, "If you will do certain things, in the enhancement of productivity, to save the Air Force money in electronic systems division component buys, we will guarantee you a 15% return on investment." It cuts down on the Air Forces problem, it cuts down Westinghouse's problem. It allows from the very beginning, and this is quoting lightly from the article, they would like Army and Navy electronic systems to also become part of this, but they are addressing the T-square, they are at the technology transfer program, right up front, with better control. They are reducing $1 billion in cost over the life of this contract, in terms of how much they are going to save in buying these component parts. They think that it will go a long way toward introducing a new concept in DOD defense contractor relationships. I can concur.

We are fooling ourselves in terms of the anti-Japanese government industry complex. We have a different view. I think opportunity in the marketplace is here and it should be here, because that does drag down costs. They're discussing this now in Congress with multi-year procurements and a number of other things. This approach is in the May issue of Government Executive Magazine. It goes into some detail about the kinds of cost savings, about the kind of control, about getting rid of the chaf early on, in terms of what do you want, what you don't want, the flawed R&D and the going back to the drawing board kind of thing. Do it right up front. You understand clearly what it is. You effect those costs savings and you get down to productivity issues. All those

are positive statements. The T-squared work, which is small, but is also a critical part of this. I think T-squared is probably correct, but also relates to the OPSEC.

The Under Secretary of Defense Research and Engineering and people in his office have been going to industry. In one specific instance, to Xerox. They have said to Xerox, you have been doing work in the TEMPEST area. Continue to do that. Go ahead and invest the capital in these things because we, DOD, will buy your products. That kind of assurance needs to be given to industry so that when they make investments, they will indeed get some return on that and they are not putting money down a sink hole. They are talking about local secure networks, etc. They want those kinds of things to be developed. They are taking their programs and their needs into the industrial environment. And I think that's working fairly well in this instance.

DOE. National Laboratories Acadamia Industry. DOE has a very fine program to date. They have published, on a monthly basis, I believe, newsletters about OPSEC, relating to espionage, hostile intelligence, and a number of other things. Their program ties together SANDIA, Lawrence Livermore, Los Alamos, etc., into the academia in the industrial site. They're doing it rather well. I think a partial model of some of what they've done up to date can be used. All these people that are mentioned are approachable. They would be happy to tell you about what they're doing, where they think they are going, their problems, how it applies to you when you go into your management and say "hey, this looks like a good idea" and they say "why is it a good idea?" and you say "dada." You have to have the kind of documentation that you can hold up or review and become conversant with.

The last thing is the OPSEC industry program. It's being done by the 902nd military intelligence group, an Army activity. They'll be happy to come out and brief you at any time. Day or night. It's a rather good program. It addresses those critical issues of cost, allocation, benefit, etc. I encourage you to make yourselves familiar with these.

Benefits and work and mutual support initiatives. I think as I just said for the Westinghouse and others, that there are reduced cost parameters. You do not fool around for a year and half and pick-out that this is not the product you wanted, or that you need to do something else. You can get very tight, up close early on, get rid of the misunderstanding and go for the product that you want to do. You can enhance productivity, and you can save yourself a lot of money early on.

Management and market requirements. As mentioned in the Xerox example, if you do not have to guess what the customer wants, or trial and error, you have a lot less investment capital at risk. You find yourself getting a return on your market investment a lot earlier and everybody is happy. So, if you can establish that kind of dialogue, you have a much better chance at success in the market place of matching the requirements to the customer. It's sort of an ABC type thing, sorry I even brought it up.

Enhanced indian security. Again from the initiation to employment, we're talking about the capability of those critical elements of each system. Each system in itself has a separate, inseparable entity being provided those kinds of things are need. VITRO Laboratories has the second largest etheran net system, after NWC's in the United States. They require cryptographic devices. Their main customer is the Electronic Systems Command. If they don't have it, they're doing their work in an environment that's unsecure, but it's going to go into a facility that is binding for secure purposes. It doesn't make sense to have a product that is perhaps already compromised, go into a secure system and be deployed. It's not going to work. So there is a capability for understanding between the defense contractor and the government rep to understand early on what is required, what's necessary, what's missing, correct those problems if any exist, and get on with business.

These are only four. There are dozens, literally dozens. Literature in this area is starting to grow rapidly. The first one is something that came out about six to seven months ago. Highly readable, it is testimoney before the Senate Governmental Affairs Committee (Committee On Governmental Affairs, Senate Report On Technology Transfer, November 15, 1982). It is relevent in that it pre-

sents 10 cases of industrial espionage security problems. It talks about the kinds of activity that we're involved in. It talks about the vulnerabilities we're looking at. It draws heavily on the unclassified CIA report. It is about 40 pages of reading and I think you will have a much better, much more clearer understanding of what this whole problem is about once you read that particular document.

JCS Publication 18, dated December 1982, is unclassified also. It is essentially the OPSEC survey guide. It tells you how to perform an OPSEC survey. What the perimeters are, what's involved, what the benefits are and how to present it. The Review of the OPSEC industry program put out by INSCOM last year had a fairly good critique of their own program. Now they've been doing it since 1977. It's a fairly mature program. It still has some problems. I won't go into those at the moment, but they're trying to correct them and they're also doing, I think, a fairly credible job of looking at themselves in terms of performance.

OPNAV instruction 3070.1, dated October 1981, is our basic documentation in the Navy for what OPSEC is and whose supposed to be performing it. There are four or five classified documents, secret level, that if you have access to them, makes extremely good reading and tells you exactly why we think OPSEC is where it's at and the way to go.

There are two benefits of this to industry defense contractors. One is a better competitive stance in the market place. We sort of touched on that. If you have an OPSEC capability and your competitors do not, and you present yourself to a defense agency and say if you have a project that needs coverage, and needs security perimeters, we've got it. I suspect you are going to have a better chance of garnering certain kinds of contracts.

Also, it's a one time investment. If you have a person who does that type of function in your organization or company, then you have an OPSEC function. You have an OSPEC focus and point of view, and the capability. You don't have to keep doing other things. You can adjust your program to the incoming contract. Dick mentioned earlier that it's a project by project basis. And that's certainly true, but the functions, the kinds of things that you do, as a gentleman or lady, gaining more and more expertise in this area, becomes a simpler and easier job and it is a corporate asset.

Defense contractors also can strengthen their in-house security capability. That's where you again use that to look at yourselves the way we do in DOD from an advesarial position. If you've got weaknesses in your programs, weaknesses in your internal controls, weaknesses in your own security functions, OPSEC is a good way to strengthen that. It gives you the ability to see yourselves as a penetrator would and to break those problems if they existed.

Possible product development. We touched on that slightly before. That is essentially, if you find that what you're doing applies to your organization there isn't that much difference. ADP physical information can be developed and sold to the Army, or sold as an asset, or sold as a program, or whatever. There is quite a possibility of developing products that have application as a marketable idea or marketable product anyway.

Cost of OPSEC? I'm not going to spend a lot of time on this. It's been overhead expense to the contractor so far. To the most extent, we'd like to see that changed if it does not get the kind of response that we'd like to see from industry. Industry is very low, and understandably, to invest a lot of money is a shakey activity. Amortized over total task or contracts, perhaps you can take a piece here, a piece there and get it paid for to some extent until you have an OPSEC capability in-house, thereby, gently easing yourself into these kinds of arenas

And thirdly, instead of an DD254 activity, you get it as a data item description on your DD1664, and then it becomes a DOD cost, which from a committee point of view, makes the most sense. It's the easiest, it's rational. I've heard figures as high as 10% of the contract cost. I think that's way out of line. I think it's much less than that.

Finally, the recommendations. I very, very strongly recommend increased DOD and Industry dialogue. If DOD doesn't come to you, perhaps you should be going to DOD. There are benefits to be derived, cost savings, and enhanced security. I don't see anything negative, except confu-

sion, and the starter problem that all programs have. The only way you're going to get through that is to start talking about it. If it's not talked about, it's not going to be addressed. If it's not addressed, it's not going to be solved. Talk about it.

Pro-active industry commitment. There are several already. In a Los Angeles paper about a month and a half ago, I believe General Electric advertised for a OPSEC officer and called it that. This is the first time I'd ever seen it. The activity out of the INSCOM briefings, and Army briefings of OPSEC industry, have gotten a lot of response from Hughes, Grumman, TRW, and a number of major defense contractors wanting to know what this is about, how they can institute it, and how they can go about selling their management on it. It's happening more and more. It's collateral and it's snowballing, but it's a low snowball now. I think it should be a faster one. I think you'll find a lot of help in documenation in this area. In fact, go out and look. It's not going to come to you as soon as you'd want it to, why don't you find out where it is.

Rapid and local development of policy. That's really a DOD or OSD function. We've had a number of pieces come out JCS, and there is more coming out. Navy, Army and Air Force all have their kinds of things. One of the Air Force comments from the last range commanders council said that they keep dragging out this elephant called operations, and they gave them a handkerchief called OPSEC and said cover the elephant. The policy needs to go into place so that we can find from each of our own projects or each of our own systems, what best to do. The overall guidance is just not there as of now. It needs to be sharper, more definative, more universal.

In the intra industry corporation, if we're working at the subcontractor level at some time in the near future, those people that are not directly in competition with you perhaps, your subcontractors or people who put out a different product, perhaps there's dialogue in that area. Pieces that they have that you don't have, and vise versa. You could make small coalitions or lightened self interest groups to pro-actively pursue this arena. It happens everyday. It should happen in this arena also.

Now more of the technology transfer, but still within this arena. The shipyard works in Russia did not have the capability of building certain things beyond a certain size. We sold them two large scale dry docks. One to the Soviets fleet in 1978, and the other one to the fleet in 1981. They now have the capability to service their aircraft carriers. They didn't have that before, and they couldn't have built it themselves. We gave it to them. Something is wrong. Half the graduate population is of non U.S. citizenship. When you get into the scientific and engineering arenas, it goes up to 80%. That's not to say that these are all hostile types, but I suspect a number of them are.

We're looking at a group of intelligence analysts whose sole function is to read, analyze and aggregate unclassified technical literature from NTIS, your engineering reports, your company reports, whatever it is, so they know what you're working on, they know where you're putting your money, they know what the future developments are, they can guess what's happening, and in many cases, they don't have to guess. That's the sole function of these people and it's happening and it's real.

The Soviet annual G&P growth is 1%-2% this coming year. They must utilize our weapons systems technology and collections techniques, otherwise, they are not going to be able to do what they want to do in this arena.

And that's the end of my statement.

*ADP SECURITY*

**John Bjork**
**Computer Security Administrator**
**Small Business Administration**
**Wash. D.C.**

My personal opinion is that because of the lack of internal controls, for federal and non-government or industry ADP systems, the potential exists for some really spectacular events. I had that statement in my mind before I got to this conference and as always, you learn a lot about other things when you come to a conference. In the session I just attended on OPSEC, I think that statement is even more appropriate now.

It's not that we haven't heard a lot about computer crime and computer problems. A cover of a Newsweek magazine, back in 1981, contained computer crime articles. Horror stories and problems are being called to our attention practically every week. You can't go to the movies without learning about how computers can be ripped off and how many problems they can cause government data bases. I understand now, although I haven't seen Superman III, there's even a computer crime in it. So what this really means is that federal data basis, and I guess for your purposes here, you would think a little bit more about OPSEC material. This presentation is just a little bit more geared to computer related crime and abuse. But since the same kind of information is contained in computer systems, the same weaknesses, the same approaches to ripping a system off can be used to get classified data or sensitive, unclassified data, as financial information.

If we try to distill the computers security problem, this is what it would look like. It's really the unauthorized intentional or accidental destruction, alteration, disclosure, or delay of those assets. Computer crime is one example that would be the unauthorized alteration. Sabotage is a big problem, especially at the technical level as we're going to see. Privacy and confidentiality problems, in this catagory of information, can add classified and unclassified unsensitive material. In other words, the unauthorized disclosure of information.

And then we have natural disasters of fire and power related problems that can make the computer system unavailable to us for use. Again, in your terms of operational security, a computer that's not to be used is just as bad as information leaking out or someone else getting the information. Denial of use can be a very offensive weapon.

Lastly, as we indicated in the initial short commentary, problems with errors and omissions are very problematic. In fact, many computer security specialists will make the comment and stand behind it that the two biggest problems with computers today are fire, and error and omissions. They're not as spectacular, but really that's where the major problems and difficulties are.

The assets at risk include: the actual equipment and the hardware, the software applications that are on the computer that do a job for the user, and the information itself, classified, personal and industry proprietary. Also the resources that are being controlled by that computer system, be it a rocket, a tank or the DOD frequency list, or the payroll, or whatever. There are also applications which are controlled like checks, requisition supplies, or make management decisions with little or no human intervention. These are the significant assets at risk.

The spreading danger of computer crime that affects these assets is quite extraordinary. Currently it's estimated to be in excess of $100 million a year. A very small part of the white collar crime growth in this country. It's also estimated that only about 15 percent of computer crimes are being reported. Banks, institutions, and companies don't want to report these types of incidents, because of what they think the stockholders will think of their security. Who wants to have stock in a company that's dumb enough to be ripped off for $2 or $3 million dollars. So, perhaps, $100 million a year is low.

There is a lot of material written about what the typical computer criminal looks like. Incidently, and I probably shouldn't make this statement, it is a male figure. Nobody seems to know, or nobody can call to mind any incident of a computer related crime that involved a woman.

The main point I would like to raise here is that this individual isn't your typical bum from skid row or some deprived individual. He's one of the best and the brightest we have, he's very well educated, and is a member normally of very good standing in society. I guess that could be said for many of the spies within our own midst that have ripped us off in the past. I don't know, maybe there is some correlation there. We will take a look at the motivation factors in just a moment.

I'd like to divide into two catagories the sources of the perpetrators.

Source Agents or Hostile Agents coming from within the computer environment and outside. Inside the computer environment, of course, you

have Systems Programmers, Programmers, Operators, Clerks, Managers, ADP Auditors and Contractors who are working on the system. These individuals have authorized access to be there. On the other side you have those individuals who are not inside your environment, they are outside your environment, and they don't have authorization even beyond the system. These are the hackers, and the external spies, the malcontents, the weirdo's, ex-employees, and ex-contractors coming back to do you in, because they have extensive knowledge of your system. There is nothing like a contractor that has worked on your system for three or four years, and then he leaves and comes through the back door to do various things, because he knows all the ways to get in.

What would some of the techniques used in some of these crimes be? What methodology is used? We are not going to dwell very much on this at all. For those of you who are not data processors, a very simple description of what a computer system could be like in block terms is as follows. There is the central processing unit, input devices, a tape drive, a card reader, and a printer. Information is stored in the disk. The communications network facilitates the transfer of the information from the computer back out to a terminal, and back and forth. Now there is extraordinary weaknesses throughout this system. And what happens is that these penetrators take different routes to get at those assets. The penetrator can take a physical route and walk in and walk out with something. The penetrator can take a technical route and come at you with technical tools. Or, take a human route and pay somebody off, or a combination of the all three. The important thing to realize is that the weaknesses exist throughout the system, the penetration attempts are going to be multifaceted; therefore, your control approach and your controls are going to have to be multifaceted throughout the system. If you don't get anything else out of my presentation today, that would be the message. Don't try to protect a computer system by encripting only, or by system high clearing everybody, or by putting a lock on the door, it's got to be a combination of several methods.

One of the methodologies that I am going to talk about is how computer crime is perpetrated and the fraudulant introduction of input documents and fraudulent manipulation of an authorized program. Now, for example, right here in Texas, in the Dallas Municipal Court System, an authorized programmer accepted a bribe and changed information on the computer system so that the warrants were not there any longer. He was authorized access to the system. All he did was do something he should not do for money.

There was also a very interesting case, where two programmers and a computer operator for the State of Maryland, University of Maryland Hospital, prepared fraudulent invoices and got themselves paid healthy amounts of money. Again, fraudulent introduction of data. The really extraordinary teaching point of that case is that they ran background checks on these individuals and they verified references. What they didn't do is check criminal records. Both of them had been indicted for embezzling a computer system. No security checks and some hospital officials' faces were red. Well, I should hope so.

Something that you do see quite often is an individual who has no business either on the system, or if he's on the system, has no business editing the files in question. The individual masquerades and gets the user ID password from somebody else. There are two more spectacular cases in the Federal Government. One very recently was at the Federal Reserve Board. A former person that worked there had access, he left, went with E. F. Hutton, dialed in with some friends ID and tried to get information on how the Federal Government was managing its money. I guess he thought E. F. Hutton could use that information. An example of masquerading as someone else. The teaching point there is you have to manage your passwords a little bit better than that. He was caught inadvertantly, of course, like all these people were.

A crack systems programmer for the Optimum Systems Incorporated in Rockville, Maryland, left the company and formed his own in the State of Virginia. He was impressed with the text editing package that was running on that computer system which was the FEA Computer (the contractor that ran the FEA Computer System) that he tried to get it himself by dialing in, using codes that he had remembered, because he was in charge of all the security codes and no one changed them

when he left. Well, somebody walking past the System Console in the computer room happened to see the password user ID combination, and said, "Hey, this guy's on vacation in Florida." They called the FBI who got a tap, and traced it back and the crack systems programmer was hauled in. They had a hard time convicting him because there's nothing to convict him on. The old problem of the data not being real data. To make a long story short, since he was in the State of Virgina, and he dialed across State lines into Maryland, he was convicted on air fraud interstate commerce. The really interesting thing here is, that he only got sixty days. We will be saying more about how computer criminals are prosecuted here within our legal system.

Another technique, of course, is passive infiltration. Most of you security types are quite aware of this. If you recall that 1981 Newsweek Cover on computer crime, in that same article was this little bit of news. Mr. O'Conner from Motorola, of course, selling encription devices. He shows how easy it is to obtain the bank transfer code by going and finding the phone link and then using an AM/FM radio and a little coil. You can listen for a change in tones until you get the data link and then record it on a cassette recorder, take it home and analyze it, and then you're home free. I think some of these techniques in the unclassified world of the military could be put to use in an interesting way, if the circuits aren't encripted. The path of infiltration is certainly another way of gaining unauthorized access to information. Another technique I think that is used very often, and it's very hard to stop this, is that of simply browsing. You don't have to be an authorized user of the system either. Dial into a system, and if you know how it works, have a scratch tape mounted and then dump it. Chances are that that site won't have any controls over that. Have another scratch tape mounted and dump it. A lot of sites don't even degauss those scratch tapes before they are being released back into the system. And so, you can have a very interesting time obtaining information by browsing.

Other ways are looking into trash dumps or trash bins where the core dumps. I remember at the Army Management System Support Agency (just a secret environment) that many times in a computer 360 we would have unclassified dumps, but there would be secret material right in the middle of it. Printouts being released as unclassified had secret information in them. Browsing is a very interesting way of getting information.

In a Wells Fargo case somebody just walked away with the source code tapes of the banks financial management packages. They don't know how damaging this has been, but it's damaging. It's critical, and it could be even worse. Again, put this in your own environment. What could be on those tapes? It may not be classified, but a combination of the information could be.

These are just a couple of other techniques. A terminal that is actually on line, but is not in use. You can connect into that line and then go ahead and operate and process, because no one's ever logged off. In a couple of instances, one is the 1979 Wells Fargo and the second one is the 1980 Morgan Guaranteed Bank, both were authorized individuals who had unauthorized bank transfers — kind of a computer related fraud. Also, there is the school situation where kids dialed into a system they had no business in, and they really crashed it techniquely. It can cause alot of problems.

The famous case of Stanley Mark Rifkin has been often referred to as a very substance of computer crime. Actually, it shows a weakness in physical access controls. The guy was a computer consultant to this bank and he had access into the area where they kept the bank codes. He gets a bank code, and gets on the phone and he calls and says transfer all this money and they say, give me the code, and so he does. They say well that's the wrong code and he says how can I get the right code. They say call this number, and he does and they give it to him, and he calls them back and they transfer the money. Then he goes and he buys these diamonds. They were all grated, and then he mixed them all together. The guy was just a total idiot. Again, caught because he was an idiot. Physical access control problems drive you crazy.

The other area I want to talk about very briefly is the explotation of Trojan Horses and other technical problems in computer systems. All these computer systems, when they were designed, had little trap doors placed in there on purpose for

debugging. These trap doors are supposed to be taken out. Unfortunately, sometimes they are not and programmers who know where they are can worm their way back into operating systems and take over the computer. There's also foubles. It's called a fouble because it's something that happens that wasn't planned, and it allows a programmer to do things he shouldn't.

Another phenomenon is the Trojan Horse. Here a programmer places a series of unauthorized code statements in the operating system and it takes this and imbeds somewhere and nobody can ever find it. It does it's dirty job and then it erases itself. These are very difficult to discover, and there is a lot of information written about this. Those of you who are interested in following-up at the DOD Level should see the people at Fort Meade. The DOD Computer Initiative Program, under Colonel Roger Shell, has done alot of work in these areas. I wanted you to be aware that these are our real weaknesses that are exploited. There is one case where a person programmed it to hide checks that he had written to himself by manipulating the computer. There is also the case of the Univac 1181 in Seattle. The extraordinary teaching point here is that this State Agency had a user design their own system, then had the programmer who designed that system operate the system, and then had the programmer who designed the system and operated the system have the authority to issue the checks. I think it's called, "Not have any separation of duties." I mean incredible. The guy wrote checks to himself, and was only caught because some clerk was looking through the invoices and happened to see an address, and he said, "that address looks familiar." Something like that is very nebulous. I talked to all the people involved, and it was an inadvertant discovery. Those are some of the methodologies used in some of these computer crimes that can be used against your systems. What are some of the motivators? Well, money is one in that none of us has enough money. The information can be very interesting to some people. That's a strong motivator. Some industries, in order to get a competitive edge, can result to industrial espionage. And, of course, I am sure that the enemy will also do the same thing. Out and out espionage against the government systems is also a motivator. Revenge is another motivator. Those of you involved in any new word processing systems, or any of the personal computers for the first time, note that first time computer users are really strange because they become very dependent on word processing. "What do you mean the Wang is down? Well, What do you mean? It's down? I can't use it? I can't finish my document I promised my boss? I don't understand what you are talking about. Fix it." "It will be down for two days." "It can't be down." And they take it and put their fist through it. Or, a personal computer is even worse. You know, they buy those things for $5,000.00. Your office buys one and then you try to use it and get dependent on it and you end up throwing it out the window because you get so mad at it. Well, that's getting back at big brother, getting back at Ma Bell, getting back at Big Blue, or IBM. All revenge syndromes. Then we have the guy who just really thinks it's a challenge. He's going to get into your system and you are going to keep him out. The hackers. There's another kind of hacker/phone freak, and this was in an issue of Technology Illustrated. They interviewed these guys up in New York. They are the new phone freaks. They used to get their jollies by dialing all the way around the world, tricking the phone company by using a little blue box that simulates the long distance codes. Well that's passe, now they get a personal computer and they are going to dial into your system, and dump it or crash it or browse through it, or do anything they can and then get out. These aren't the criminals, but when your data base has been violated it's kind of like being robbed. You know, you don't want these guys in there and want to figure a way to keep them out.

Those are some motivators. We took a look at what the problem was, and who's doing it, where they were, what are some of the techniques they used, and what some of the motivators were. Well, how in the world can they do all these things, what are some of the reasons why computers are so irresistable, why do these things happen, why do computer security officers get gray hair prematurely? One is the technology involved. Take the case of an original Heniak thirty ton computer. It's being replaced by a brand new Sperry 1160, a little bit smaller. The point here is that technology with it's speed of operation and tremendous amounts of storage, not only has made the computer a tool for us, but it's made it a target for

other people. And it's extraordinarily easy to manipulate these computers to your own untorn ends.

Another general reason contributing to computer crime and abuse, and espionage by computer is a total complexity of the data processing environment. The software that comes with the computer, that runs the computer, that manages it contains millions and millions of lines of code. No one person could possibly understand it. There are a lot of holes in it. If you have ever been in a big computer center, to see the complexity, you can imagine how easy, at nana second speed, things can go wrong.

There's a tendancy for most vendors to provide an extraordinary amount of power to run that computer for programmers and users. The problem here is that they don't always need it. If they take advantage of those tools, they can bypass security controls.

More and more people are getting involved in data processing. Within organizations, everybody's got to have a terminal with more and more power. The personal computer probably is the single most glaring reason why the computer is going to be "the thing" in the next twenty years. These companies are making computers available that have power that, just a few years ago, was unheard of. Everybody's going to have a home computer complete with telecommunications capability. You can dial in any place you want. We have, at our agency, one of the new compus grids. A 380K, complete teleprocessing, integrated software, formats that downloaded systems anyway I want. It's just incredible. A white collar criminal's dream can come true. Management is giving every manager a terminal and let him interact with the computer. To hell with the data processors. You're seeing this in the Data Processing news now. Forget about the data processors, they never could solve your problems anyway. You get our personal computer with our software, you access that mainframe, you do what you want with it, update it and so on.

Data processing, the data processing shop, the computer people, are operations oriented. They are getting paid to get the job done, not to protect data.

Managers are not security conscience enough about computers. They are getting graded on performance, and they just don't have time for security. "Who wants it?" "Who wants to put up with that overhead?" "Document control, batch control, uh, yuk." Well, nor does a data processing manager want to do all that stuff, either. Nor do users, nobody wants to do it all, or any of it. Well, that's what happens. Dependence on the computer itself. We are so dependent upon data processing today that if we don't have it, church is out. Computer crime is very glamorous, and it's very difficult to prosecute a criminal for computer fraud. I mean, now is the time to do it before the Federal Computer Crime Act goes into being. I understand, it's going to be reintroduced finally.

Those are some of the reasons why computer systems are such great targets today. What happens is there are weaknesses throughout the computer system. Let's just go over where they are so you are familar with that, if you haven't thought about that already. A good example of a vulnerability is a computer terminal that has no hardware identification features, so you don't know when someone's dialing into your system, if that hardware belongs in your environment. A dial up terminal in itself is a vulnerability. The first catagory, again operating system flaws, there is alot of weaknesses in that area. Many times applications are planned and designed and there's no emphasis, or interest, or any word given to the security controls. Who can access the files? The files you find, alot of times, show the data sets don't even have password protection on it. There is no set data sensitivity evaluation. Nobody knows how sensitive it is, there is no sharing requirements stated, so who cares? It's out there ready to be exploited.

Physical access controls on the computer room, remote terminal areas, sensitive system programming areas, ADP Media. I mentioned that incident about the tapes. Also, reports, are they sensitive? Well, if they are, where are the markings? And, if they are marked, is someone checking the middle of them? And, how about IO control? Who can pick them up? Who can send them out? Who can destroy them? And, speaking of destruction, how is the destruction of this material handled?

Very interesting, if you are going to penetrate a computer sytem, the first thing I would do is go look in the back of the building to find out all these nice little source listings that give me all the log on protocals and probably the passwords. Then I'm home free, I combine it with a technical penetration and at night and your asleep, into your data base I'll creep.

Personnel security. There is very special concern in data processing, and within the Federal Government and contractors. If you are a contractor, you are bound by the Office of Personnel Management AP Personnel Security System. There are three catagories depending upon how sensitive the positon is. Again, teleprocessing, if you don't have adequate controls there, this is what can happen. Some of the weaknesses include: No log on passwords, terminals not being able to be identified in a hardware, dial up terminals themselves, and of course the Soviet Agent ready to grab all that sensitive tempest material that we spend millions of dollars protecting against.

Also, there are alot of problems in the computer environment. We won't spend too much time on this, but alot of errors, and omissions occur because of crashes, fade outs, brown outs, surges, and so on. And of course, inadequate detection methods for fires can cause bad things to happen. Well, all is not lost.

Suppose I say that all these weaknesses that exsist in these computer systems can be reduced, in a cost effective way, in a manner appropriate for your own environment.

Does anybody know the methodology we would use?

Risk assessment! Right? You must of heard that before. You have got DOD Directive 5220,2f, and it's many little subsequent documents. You should have OMB circular 871 dated June 1978. Really, make sure that all Federal Agencies have responsibility for computer security, personnel security screening program, control of the software, risk analysis audit and a contingency plan.

If you are building a security program, the only way you are ever going to get a handle on the problem, even if it's classified, or if it is business data, or what ever your environment is to establish a formal program. This program prevents the trends from occuring, detects problems, minimizes the impact and then allows you to recover if all of your other safeguards have failed.

Let's take a real brief moment to take a look at the systems approach. When you analyze your system, you identify all the weaknesses in all areas such as operating systems, remote terminals, physical access controls and media protection and postulate some threats and what could go wrong if these threats, if these weaknesses were exploited? Identify countermeasures, get some cost effective fixes going, get management to sign-off and then implement them, and monitor them, and back and forth. Would you have to go through this iteration again. Let's say you did this this year. When would you have to go through it again?

Certainly, if you have got significant changes to hardware, software, or if you have new systems. It should be done all the time anyway, but I mean, if your in a file oriented system and suddenly you go to a massive data base management system, or adding dial up terminals, this should be re-evaluated.

So, there you are ready to implement your controls, and keep in mind they have got to be in all these areas. You know, you just don't want them in just one area. Above all, have a competent, well trained, energetic, computer security manager to do it all.

Somethings that you are going to want to do now in the technical area are making sure that users are identified and authenticated, that their paths to processes and resources are controlled and that if there happens to be terminals involved you can use a neat little profile there, of certain people. Certain resources are accesses through certain functions only by certain terminals which pick all the known operating system flaws that you can find. A good source for those flaws is to go to the user groups of the system involved. Guide and share. You certainly want to have a mechanism using the systems management facility of each computer in IBM to audit what is going on in the computer system, provide a detection and response mechanism, based on

utilizing that system management tool. It comes with the operating system software, so all you have to do is use it.

Physical access controls. Immediate protection controls. Again you can use card key systems, tape management systems with tapes, effective IO controls for printouts, and have real nice tight, effective physical and media protection programs. In the area of more remote access security, certainly take a look at encription, if the risk assessment justifies it, and just a couple other tricks. You try to keep dial up terminals off, but if you can't, one thing you can do is put little chips into these terminals. Some terminals, I know Texas Instrument Silent 700 can do this at a cost of about $150. You program your front-end communciations processor to interrogate that chip so anytime anybody dials in to your system, there is a physical handshaking there, even before the password exchange. What that does for you is it keeps all these hackers and weirdos from buying PC's or other terminals like an Osborn with a 3270 emulation package to come in and do alot of damage, because they don't have a chip. There is no chip on there so they can't get in. Certainly, a password system is good. Another way is terminal computer call back. You have dial up terminals that the people dial in to a scheduler and you have him call the person back. Nobody dials in automatically. There is also a couple of physical security devices that we are evaluating that are interposed between the dialing ports and the phone line. It provides a second level of password control which you can change alot easier than system passwords, especially if you have got a password control system that the users manage themselves. I have a nice ADP Personnel Security Enhancement Program. There are many different techniques you can use there. They are written up in the literature. On investigations, don't forget to check criminal records and education for those people, and if you ever terminate anyone for cause, don't keep them on the job for 4 or 5 weeks. There are many horror stories about people being terminated like tape librarians and so on, and they were able to wreck their vengence before they were let out the door. So if you have sensitive people they shouldn't be kept on the job if they are being terminated for cause.

Physical security for computer systems. In this regard I am refering to the controls for power monitoring and fire detection and so on. There is a lot of literature on that.

Contingency Planning. Having an effective contingency plan is an absolute must. Even if it is just making sure that your critical systems, are backed-up at least daily, and stored for God's sake off-site, so that if a fire were to destroy your center, you could at least survive. Let me leave you with a word of caution to try to run those tapes occasionally. I've seen cases where people had an effective back-up program, only to learn to their horror that they could not read those back-up tapes. There was something wrong in the back-up program, the oxide was coming off the tapes. You know, there are all kinds of different reasons. Don't use chip tapes for back-up tapes. Use the absolute best you can get. Test them continually. Because, if you don't have that computer, or those critical systems available, that can be really a very serious problem. It can bring a company right to its knees. If we built our program we put all these hot controls in there to reduce those vulnerabilities, to keep these hackers and crooks, malcontents, and spies out of your system. Thank you.

Q: If you're processing classified information inside your building, how can I get at it if I am outside?

A: Well, I would have to come over and take a look at your system, but one way again is this tempest thing. That can be done. Compromising eminations can be gleaned.

*GAO SECURITY REVIEW UPDATE*

**Irving Boker**
**U.S. GENERAL ACCOUNTING OFFICE**

Before proceeding I'd like to clarify two common misconceptions. First — we work for GAO not GSA. GSA is the General Services Administration. We like to think of ourselves as the government's house cleaner. GSA is the government's housekeeper. Second, GAO does not stand for Government Accounting Office. It stands for General Accounting Office.

Those of you at last year's seminar in Orlando may recall that I discussed carve-out contracts. I

never anticipated talking so much on this one subject, but that review took us a long time to do because of access to records problems and it was a rather difficult job to get involved in. But it is the subject of continuing interest to many security professionals in industry and in government. Last year, I covered the background of special access programs, carve-out controls and some of the peculiar terminology associated with both. I also covered our approach to the job, some problems that we encountered and a brief description of some of our findings. Today I will discuss some of the findings in more detail, our recommendations to the Secretary of Defense, and to a limited extent DOD's reaction. As Jack Robinson so aptly put it in the latest addition of the bulletin, DOD carved-out its comments from our report. That report, there are some copies in the back of the room, is that further improvements are needed in Department of Defense carve-out and Special Access contracts. It was issued February 18th and these copies are available to everybody. If there's not enough back there we will certainly provide any additional copies you may need. In view of this the carve-out comments are in a report, same title but marked For Official Use Only. There's a little story behind this. When DOD got our advance report for comment, which is our policy, they were talking about classifying our report and I said if you classify it I can guarantee you a Congressional hearing. So I asked, "What is it you want classified?" They said it had a paragraph on what the intelligence community is doing and it was marked "confidential" in their comments. I said "Well take that paragraph out." Well, they did, and I said we want the report or the comments For Official Use Only which means that it can be used within government or given to contractors that have clear facilities. So if anybody that didn't get a copy of this would like one, if you'd see me after the meeting or the break this morning, we'll be happy to give you copies if you properly identify yourself or I'll send you some in case we run out. To be sure there's no misunderstanding about what a carve-out Contract is, it is a special access contract for which the Defense Investigative Service has been relieved of inspection responsibility under the Defense Industrial Security Program. The DOD component that awarded the contract assumes responsibility for security inspections. One other point probably requires a little clarification. There are two types of carve-out Contracts. The first type involves intelligence or intelligence related information. Such information is called sensitive compartmented information (SCI) and it is kept in a sensitive compartmented information facility, (SCIF). The second type of carve-out Contract involves intelligence related information, such as some of the research and development programs. We had 4 general findings in our report. The first one was oversight procedures needed for carve-out contracts. We concluded that better oversight procedures were needed for carve-out Contracts because there was an inconsistency in the establisment of many non-SCI carve-out Contracts and the security clearance level of some contractor employees with access to contract information and some contracts were carved-out for reasons other than security. We call those contracts SOB's. Many non-SCI carve-out Contracts were classified at the SECRET level which meant that many contractor employees with only SECRET clearance had access to contract data. Since SECRET clearances for contractor personnel generally are granted on the basis of only a national agency check it seemed inconsistant to keep out DIS inspectors who have TOP SECRET clearances granted on the basis of a favorable background investigation. The situation became a little more disturbing when we tried to determine how many contractor employees with only SECRET clearances had access to the contracts. The military services told us about 39,000 contractor employees had been granted access to NON-SCI contracts, and over 13,000, 1/3 had SECRET clearances. One DOD official who will remain nameless, estimated the number of contractor employees with NON-SCI access was substantially higher, close to 100,000 more than the 39,000 figure given us. I don't mean to imply that headquarters offices of the military services would give us incorrect information. They would never do that. The truth of the matter is that the headquarters offices of the services probably did not, and possibly still do not know the existence of all NON-SCI carve-out Contracts. Several contractor and DOD officials told us that they thought that carve-out Contracts were being used to expedite procurements and facilitate sole source awards. We found several examples that illustrate that security probably was not the primary justification for contracts being carved-out. One contractor told us that the reason for one service carve-

out Contract was to keep another service from knowing of the existence of the contract and its sponsor, rather than to ensure the security of the information. Another contractor told us that the purpose of one carve-out Contract was to evaluate the work being done by other contractors. Two contractors said that for their contracts only the contract documents themselves were carved-out. The statements of work and documents related to contract performance were not carved-out. One of the contractors thought that the reason for this unusual arrangement was to preclude someone from identifying the military service involved and the amount of money being spent. Another contractor said that a contract was carved-out to expedite procurement. The contractor told us that, initially, precontract award lead time was estimated to be two years. After the contract was carved-out, the lead time was reduced to six months. In August 1982, DOD revised the Information Security Program Regulation, the well known 5200.1R. Among the many changes were several improvements involving carve-out Contracts. First each DOD component will be required to establish a single point of contact for security control and administration of all special access programs and carve-out contracts. Second, use of carve-out contracts that do not support properly approved special access programs is prohibited. Third, each component is required to establish a written security plan for each carve-out contract. We fully support those revisions. However, we believe that some additional controls are needed.

So we recommended that the Secretary of Defense revise the Information Security Program Regulation to require all components to annually (1) inventory and report the status of all carve-out contracts to the Deputy Under the Secretary of Defense for Policy. And (2) revalidate the need for renewed contracts or contracts that extend for more than one year. We also recommend that the Secretary require the office of the Deputy Under Secretary of Defense for Policy to make periodic inspections of component's central offices to evaluate compliance with the regulation.

DOD agreed with two of the recommendations but did not agree with the need to revalidate the justification for renewed contracts or contracts that extend for more than one year. As an alternative, DOD suggested that the Defense Acquisition Regulations be revised to insure that carve-out status is reserved exclusively for contracts which meet the security test. We support a revision of the Defense Acquisition Regulations, but we still believe that revalidation is needed because we saw one contract that was awarded for a ten year period, and several that were renewed annually by an amendment to the contract.

A second finding is that improvement was needed in implementation of uniform SCIF construction standards. On the basis of the SCIF's that we visited, physical protection for SCI appeared to be more than adequate. In many cases the SCIF's resembled what you'd expect to find at Fort Knox, Kentucky. At the other end of the spectrum we saw less auspicious facilities, many in commercial buildings without guard service and restricted building access found at the Fort Knox's. Although the Defense Intelligence Agency has issued minimum SCIF construction standards for DOD components to follow, the military services were occasionally constructing SCIF's based on higher standards. Design and construction or alteration of the SCIF's was not preceded by a threat analysis. As I mentioned last year, the cost of SCIF's can range from one room 9x12 ft. to many rooms comprising about 40,000 sq. ft. In some cases the SCIF's appear to be little more than storage areas for SCI. In other cases, they appeared to be beehives of activity where outsiders, such as auditors, were treated like they had the plague.

Because of the inconsistency in implementing SCIF construction standards, we recommended that the Defense Intelligence Agency regulations be revised to require that a threat analysis be made before a SCIF is constructed or altered or an existing facility is approved for use as a DOD SCIF. We also recommended that the Defense Intelligence Agency be made responsible for approving all industry facilities proposed for use as DOD SCIF's.

DOD agreed with our finding but not our recommendations and proposed some revisions to the regulations. The revisions are good but we don't believe they go far enough to correct the deficiencies that we observed.

Our third finding was that there was a need for

one group in DOD to inspect all SCIF's and special access contracts. We concluded that centralized inspections of SCIF's and special access contracts by DIS could eliminate or substantially reduce the number of carve-out contracts, insure that all contractor SCIF's and documents therein, are being inspected at least annually, and eliminate or reduce duplicate inspections of the same SCIF's. DIS already makes security inspections for some special access contracts and we see no reason why DIS shouldn't be inspecting most existing carve-out contracts. Of course, if DIS does the inspecting the contracts are no longer carve-outs. They are just special access contracts and DIS already inspects a number of special access contracts. Special access contract documents could still be given extra protection by being stored in SCIF's and restricted personnel access could still be maintained. Many of the SCIF's could be inspected when DIS makes its semi-annual inspection of contractor facilities. One of the objections to having DIS inspect carve-out Contracts is that it would proliferate access beyond the minimum number of persons that need to know about a contract. The logic to that objection is really incredible. DIS has a total of about 175 inspectors. In industry anywhere from 39,000 to 150,000 individuals have special access authorizations. If DIS were permitted to make security inspections of SCIF's, in many cases the SCIF's would be inspected more often than they currently are. In most cases the military special security officers, the SSO's, inspect the SCIF's on annual basis. DIS would be in there twice a year. One of the primary purposes of a SCIF is for the storage of SCI. Every SCIF has a DOD component that is the SCIF sponsor. That component, be it Army, Navy or Air Force, at one time or another, had the only or most of the SCI contracts with the contractor. The SCIF's sponsor is responsible for making the annual security inspections which generally include physical security and an accountablity check of the sponsors documents stored in the SCIF. Other services or DOD components are permitted to use the SCIF for storing their SCI documents relating to contract work. These other groups are known as tenants. The SCIF sponsor during the annual inspection does not test the accountability system for a tenant's SCI documents. Unfortunately some of the tenants in some cases also are not testing the system applicable to their SCI documents. Several contractors told us that the contract monitors either had never inspected SCI documents or had done so infrequently. In one case contract documents had not been inspected by a military tenant for six years. Another contractor said that a military tenant had not inspected their documents for five years. A few contractors told us that to facilitate working with some contracts, documents not requiring special access control were stored in the SCIF's along with documents that required special handling. DOD components inspected the special access documents but they did not inspect the other group. Since DIS inspectors are not allowed to inspect the SCIF's or their contents, the nonspecial access were not inspected by anyone. We also noted a few cases of duplicate inspections even though the SCIF's sponsor had made a physical inspection of a SCIF, the inspection was duplicated a short time later by a tenant. So we recommend that the Secretary of Defense make DIS responsible for inspecting all DOD sponsored contractor SCIF's and for verifing accountability for all contract documents maintained in those SCIF's, and SCIF's sponsored by other agencies. The Department of Defense did not agree with our recommendation and gave a number of reasons for its position. One of the reasons I mentioned earlier: the proliferation of access beyond the minimum number of persons for the need to know. Some of the other reasons were that DIS is not staffed to assume the added work; DIS inspectors would require training because of the various security requirements unique to special access contracts and the designated security officer with program familiarity is better equipped to make inspections than the DIS inspector. There may be a small degree of merit in some of the objections raised by DOD. I can sum up the department's position with just one word, hogwash! Or to use the mash expression, cowchips! If functional responsibility for inspecting special access contracts is transferred to DIS, there is no reason why the bodies cannot be transferred with the function. In other words the SSO's could be transferred over to DIS. We do not believe that program familiarity is a prerequisite for the retention of the security cognizance. That's probably the same argument that was used fifteen years ago when security cognizance with the Defense Industrial Security Program was centralized. While standards have been established for the added protection of SCI, no standards have been established for protecting

the NON-SCI's special access data. We believe that standards need to be established for that information which requires protection over and above the requirements included in the Industrial Security Manual. We believe that DIS should make the inspections for compliance with those standards. Our last finding was improvement was needed in the advance approval of special access requests that requires special background investigations. Some contractors, were submitting requests in excess of their specific needs for special access authorizations that require special background investigations by DIS. The excess requests were submitted to fill positions in anticipation of new contracts and employee turnover. This practice which is contrary to DOD instructions could be eliminated or curtailed by strict enforcement of the requirement for DOD advance approval of contractors' request for the special access authorizations. The successful completion of the special background investigation is a prerequisite for access to all SCI contracts and to many Non-SCI special access contracts. The excess requests have increased the DIS workload and contributed to delays in the processing of all requests for investigations. We recommend that the Secretary of Defense issue instructions that will require advance approval by DOD of contractors' request for special access authorizations for employees who will be working on NON-SCI special access contracts. We recommend that DIS return to contractors any requests for special access authorizations that do not contain the advance approval of the cognizant DOD component. We recommend that the secretary remind DOD components of their responsibility to review and approve (in a timely manner) contractor nominees for all special access authorizations. The Department of Defense agreed with our findings and recommendations and said that corrective action was being taken.

I consider it a privilage to be a member of NCMS and I consider it an honor to be elected to the Board of Directors. I will try to fullfil the objectives of the society because they are consistent with the objectives of GAO in the security information area. That's to improve the protection of National Security Information. I will close with a borrowed quotation from Abraham Lincoln only changing the pronoun. "We have always wanted to deal with everyone we meet candidly and honestly. If we have made any assertion not warranted by facts and it is pointed out to us, we will withdraw it cheerfully". Thank you very much.

## *NCMS INTERNATIONAL AFFAIRS COMMITTEE REPORT*

**Jim Bagley**
**President**
**R. B. Associates**

I am always reminded when I come to these seminars, and I have unfortunately only missed one, of the change in the atmosphere. About fifteen years ago you would look out across the room and you see "The Gerryatrics Set". Mostly male, rather old, somewhat set in their ways and yet I can remember being on a panel with Sheila a number of years ago in which I said, "Would it not be nice, if at least a gender would change a little bit." But looking around the room I see roughly half the people are in fact female. There is a substantial number of other people here. We have other nationalities, ethnic backgrounds and what have you. It is indeed refreshing. This is the first of what I hope will be a continuing dialogue on the problems of dealing with international problems. Quite candidly I fell into this business, quite by accident. I can say that Liz Heinbuch recommended me to a general friend of hers and here I am doing this business. Today I would like to discuss particularly how the committee came to be and how U.S. companies operate within Europe, and again I stress, I am talking Europe and the United Kingdom. I am not talking about your activities throughout other parts of the world, the Mid-East, Africa, Far-East and what have you. I am stressing this entirely to Europe, the security agreements which are in place, how foreign companies operate within the United States, where we are and where I think we should be going. First the committee. As was announced the committee is in place. And one of the real roles that we will have, I think is to cooperate with other national bodies which may exist, so that there can be an interchange of information, intercommunication dialogue or however you wish to define it. And, as there are many people in this room at this minute who have problems of real input, I hope that the committee then can assist you in some of your problems. Now the committee members of which I am very proud of. Bob

Grogen from Canada, John McMichael the Chairman of the UK Guild of Security Controllers, Bob White from Cincinnati Electronics, Larry Howe from SAI, Dean Richardson from Texas Instruments, Ed Silver from Hughes Aircraft Company, and Chuck Fainsbert from Microwave Semiconductors Corporation. Our first formal get together was yesterday. And we agreed generally that there are problems which need attention and that NCMS can in its historic role do something about it. That throughout the years and in the future, subjects should be developed, presented, issues raised and possible solutions presented to the appproppriate bodies. That the issues of fairness, equity, reasonably equal treatment, between companies of those countries with which the United States has reciprocal agreements should be addressed. From background, of course, you know that NCMS has been involved in this kind of business since the beginning. If you would look back to the earliest seminars, seminar #1 for example, we discussed then the arms control problems and we discussed international relations. Throughout the years we've discussed such subjects as; and this may surprise some of the newcomers: classification in Russia, the British officials secrets act, classification practices of foreign governments and there have been many other subjects. Because there was no other vehicle at that time, Bob Grogan's immediate predecessor, Stan Jenkins, was made an honorary member of this society in 1972. Since then, of course, the bylaws of this society have been changed so that membership can be permitted to people who are representatives of those countries with which the United States does have agreements. According to the manual now, and I emphasize the manual, there are three such reciprocal agreements in existence with the UK, Canada, and the Federal Republic of Germany. I know there are others, but the manual only speaks of three. So this is some of the small background. But, there are problems and at the outset I would like to ask those present two questions. Of the Companies present, how many of you, and if you would please show your hands, deal in, have subsidiaries in, either the UK, Canada or in Europe? Would you please raise your hands? There is a substantial number, ok. For the user agencies present, would those of you raise your hands who have experience with or deal with companies that have reciprocal clearances? Would you put your hands up please? There are a few. But then, how do UK companies and US companies, do business in the UK or in Canada? You might remember that at the Orlando seminar last year, I had the honor of chairing a panel in which, Bob Grogen, Edgar Hill and our esteemed Art Van-Cook represented the views of their governments. On the other side there was Jim Wyatt from Marconi and Bob White from Cincinnati and John McMichael from the UK who said this is the way the world is and of course since we knew then, never the twain shall meet. But, I'd like to sum up some of the things that happened as a result of that panel. The representatives of the Governments did present to the attendees the policies and on the other side we heard the horror stories. In the best interests of promoting the learning process, and this is why we're here, it must be accepted that there are and will continue to be, differences in the manner in which agreements are implemented by the governments and these differences are based on laws, tradition, practices and customs. For example, in the U.S. the contracting procedures are prescribed by law and regulation. The authority for example of a procurement activity to advertise or not advertise, its quite limited. In the UK and Canada they have much, much wider authority. In the UK and Canada there is no equivalent to our DOD security agreement the DD form 441. In the UK and Canada the security rules are prescribed in the contractural basis generally, and could vary from contract to contract. In those countries a firm whether UK or foreign, does not have to seek a formal facility clearance before it can be considered for classified work and of course as you know under the US rules a firm must first be sponsored by a procurement activity. In the case of a foreign firm, the UK or Canada seek confirmation of the firm's security status, security assurance, if you will, from the country of origin. Now the US does have specific access limitations for firms with reciprocal clearances, Restricted Data, Pact information, COMSEC, etc. The UK and Canada have no formal equivalent of those limitations which prohibit the release of certain categories of information from being released to a foreign owned company qualified to do classified work in their countries. There may however, and there always is some information which is entirely proprietary to the country. UK Eyes only, Canada Eyes only, hundreds of cases of U.S. Eyes only, not withstanding of course Air Force, Navy, and

Army Eyes only. But a US subsidiary operating in a foreign country, may and does have access to the highest classification of information. For example, a US company beat out Marconi recently in being awarded a very highly classified COMSEC contract. It does happpen. On the US side the reciprocal clearance produces problems. When the clearance is granted, and I will not go through the process by which it is granted, the firms ability to get new business is jeapordized because it is in fact cut off from access to information, access to seminars and access to procurement information. It does happen and there are people in this room at this minute to which it applies. Therefore, if it is the policy of the United States to further international cooperation and to implement the agreement which it has signed, then something must well be looked at. So, it leaves inevitably to several questions. Is the DOD reciprocal clearance a valid instrument for doing business? Is not foreign disclosure an important, or the most important ingredient of a program? At what point should the foreign disclosure decisions be made? Does a subordinate command have the authority to reverse the decision of higher authority? If the DOD policies are considered viable, but the implementation of that policy by a subordinate is unacceptable, should those policies be changed? Is the industrial security program which was established to provide a single DOD industry system workable and capable of handling these problems? Now, where are we? The agreements are in place, the problems are many. From my experience, I would emphasize very strongly that the attitude of the Defense Investigative Service (DIS) and the attitude of the people within the DIS regions is superb. They are positive, they are cooperative and they are helpful. The problem of course is with the user agencies who follow the Industrial Security Manual (ISM). In fact neither the Army the Air Force or the Navy, do agree, and do not follow the ISM procedures with respect to handling companies having reciprocal clearances. Some examples: in many instances activities will require that a clearance be processed through the appropriate embassy, rather than following the procedures that are set out in the manual. Willey nilley they decide access to meetings because foreign disclosure decisions have not been made. You might know that I've been around long enough, that there was a time at least that many of the major simposia taking place, that those decisions were made up front, at the time a paper was accepted. Was it releasable? Was it not releasable? If so, what was or what was not releasable? Access to bid and proposal information is routinely denied. I have frankly hundreds of examples. The most frequent causes for denial is that the holder of a reciprocal clearance is a foreigner, a foreign national. Information is denied because the information has not been specifically released to the country requesting it. All that means, ladies and gentlemen, is that someone hasn't found out what the disclosure decision was or has it been made or will they do something about it. It's a very convenient excuse. In one case, I know this personally, the company was told go to DIS, it's their problem, it's in their manual. But I have yet to find out that DIS is a foreign disclosure authority. Those authorities, those decisions are in fact the user agency decision. It's not DIS, but they are being used as a scapegoat. The DD254 frequently uses a phrase quote "Dissemination to foreign nationals require a reciprocal clearance. Clearances are not authorized without the specific approval of blank." All that is suppose to mean, is should you go back to the component commander or what have you, and find out can it be done. The simple answer, a practical answer is to follow the ISM. For the most part it is a workable document. I would say that the second, the key that we have been talking about for twenty years in this organization, is proper classification gudiance. Guidance to me has always meant that the decision was made whether something was or wasn't releasable. You make it up front. And I would again refer to the famous bible 5200.1R's and its appropriate regulation implementations. The third thing is that foreign disclosure decisions are made in accordance with regulations which now exist and generally this is implemented by the military departments, at the systems command level and rarely below that. When I see as I do, foreign disclosure decisions being made by a rather low level installation commander or porcurement activity then I can assure you it will challenged. Fourth, the old bugaboo, the term NOFORN is being used frequently, not withstanding the fact that the definitions have changed and the body of information to which it applies is relatively narrow. And finally the US does have industrial security agreements with several countries. Please be aware, that negative

decisions will be challenged to the highest levels of the government. Such challenges have already been made, if you have been reading the papers in the last couple of months, and will continue to be made. And what would you think to go back to the first question I asked. If the companies involved doing business in foreign countries were given the same treatment as their companies operating in the U.S. I think it would hit about .10 on the Richter Scale. In conclusion I have reported conditions as they are. If the U.S. desires cooperation to continue then the buyers of the goods must get their acts together. Remember too, that militarily useful technology is not solely american. Other countries do have highly superior technology in products in many areas of need. This fact has been made in testimony by several secretaries of Defense and several Deputy Directors for Research and Engineering over the last few years. And further it is my judgement that our allies are equally concerned about the unauthorized dissemination of technology. For the last couple of hundred years, as you know, they have been rather vulnerable and we have seen lots and lots of wars over long periods of time. They do have a point.

## *OPERATION EXODUS*

**E. Meade Feild**
**U.S. Customs Department**

I want to start off with giving you a brief introduction to our program. As all of you know, it's been in force for about two years, since about 1980. It now has an official name called, Operation Exodus. We've received, as they say in the theatre, mixed reviews — according to which theatre you attend. On the negative side, a prestigous academic society has written us a letter and it said that we are causing quote, "A chilling affect" on academic exchange. This occurred when we tossed, as we say in customs — searched or tossed, several departing Chinese graduate engineering students to see if they had any technical data with them. A very well known newspaper has labelled us as bandits and thugs. The newspaper was PRAVDA. The incident was, when we searched their aeroflight plane, about a year and a half ago at Dallas airport. That caused quite a stir. I don't know if you remember it or not. The Soviet Vice Ambassador came out and we informed him that his airline was no different than Pan Am or Air New Guinea, or whatever else. He took exception to it, but we seized his goods anyway.

We have a pending bill, right now, in Congress, that if passed would strip all our funding for export enforcement. We receive nasty letters every day. And then we have the Commerce Department — and I'll save that story for another day.

On the positive side, we've established strong and continuing relations with DOD, the CIA, NSA, and FBI, and they continue to strengthen and build every day. We have gotten increased funding for this fiscal year, mainly through the efforts of DOD. We are getting generally favorable support from the Hi Tech industry, and I'll get into that a little bit later.

On the other side of the Congress, there is a bill pending to give us exclusive enforcement with the Export Administration Act. So, we're damned on one side and favored on the other side. It's kind of interesting. We write a lot of memos about this.

Now our presentation is going to cover 5 major points: A quick overview of what our program is ... and then the program in detail ... the results that we are having ... problems that we are having ... and the help that we need from you, particularly the industry.

The Customs Export Control Program is known as Operation Exodus, as most of you are probably familiar with. A primary goal is to fort the elicit transfer of critical and high technology to the Soviet and Sino blocs. Other goals include stopping elicit munitions in technology shipments to countries undergoing terrorists or insurgent activities, and to countries that support these activities, such as Lybia and Iran. Also, attention is given to stopping elicit munitions and technology shipments to countries that are embargoed for foreign policy purposes, such as South Africa. The program is being given the highest attention by both Treasury our parent and Customs Management, and also of course, the administration itself. We coordinate our program closely with

other export control agencies and with intelligence agencies, both here and abroad. The program is multifaceted. We have inspections of goods being exported. We investigate allegations of the export laws. And we develop a news intelligence, both from our own sources and from the other agencies that we work with. The formal operation, Operation Exodus, was conceived on October 1st, or launched on October 1st, 1981. Basically, we enforce 2 laws, which I think most of you are familiar with. I will just briefly go over them for you.

These laws are enacted by Congress over the past to prohibit or restrict the export from the country of material and goods that may be detrimental to our foreign policy or our national security interests. Currently there are two main laws. The first, The Arms Export Control Act, and the second is The Export Administration Act. Let me go back to the first one, The Arms Export Control Act.

For you lawyers in the crowd, you can cite this as 22 USC 2778. And it concerns the export law of munitions items, and these range from 22 caliber bullets all the way up to the most sophisticated state-of-the-art military radar and laser systems. There is a companion set of regulations known as ITAR, or International Traffic in Arms Regulations. The regulations define the munitions items and the licensing procedures. In general, most munitions need to be licensed before they can be exported. Now the law, the licensing, and the administration is done by the Department of State and the Office of Munitions Control. Later on this morning there will be a gentlemen from that office here. We, meaning the Custom Service, is delegated to enforce the law.

The second main law is The Export Administration Act of 1979. Again, for the lawyers, that's cited as 50 USC Appendix 2401. Except for munitions, this is the primary export law. Almost all exports are governed by this law. There is a companion set of regulations for this law, known as the Export Control Regulations. Now as you all are probably aware, there are certain items that need validated licenses for export, known commonly as dual used items. They have both civilian and military applicability.

These items are found on what is known as the Commodities Control List, or the CCL. And, it includes technical data, not only hardware, but the technical data. And I'll get into this a little bit later also. We enforce the law, and of course it includes making sure that technical data is licensed when it leaves.

The law is administered and enforced by the Department of Commerce. Customs also has enciliary enforcement of it because we have enforcement powers, such as arrest, search and seizure powers, whereas, the Commerce officers do not.

Thirdly, I just want to touch upon the Espionage Statutes which are enforced by the FBI. If we come across a transfer or elicit export of classified material, be it documents or actual hardware, we call in the FBI, because this is an espionage violation. We usually work the case jointly with them. The individual or the corporation can be charged both for the Espionage and the export laws. As we are getting into this program more and more, we are becoming jointly meshed with the FBI, not only in this, but also in their foreign counter intelligence. Because it is just very different, different colors of grey between ours and theirs.

The Exodus Program is physically located at 42 different ports, and at Headquarters. Now when I say the program, I mean teams, the Exodus teams, which I will describe in a second. Also, however, at every port in the country export enforcement is being emphasized. So there may not be an actual Exodus team at a certain port, but we do stress to our Customs inspectors to make export inspections. This will continue on down the line. The Exodus Program, I would just like to say, is not one of these programs that come up today, we can run it for awhile and then we drop it, which is so typical of a lot of government agencies. This program is here to stay. And it's not going to be dropped. And if we lose funding in this area, we will then probably realocate our budget to keep it going, because it is being stressed from the White House on down.

The Exodus team members consist of three types of customs officers, the Customs inspec-

tors, the patrol officers, and the special agents. They are coordinated at each one of these ports by what is known as a port coordinator, who is a special agent. He has the overall responsibility for coordinating the inspections and the investigation and the intelligence collection and dissemination into a unified export control program for the particular port. The size of the team depends upon the location of the port and the volume of exports. The technical assistance is rendered by other customs officers and other government officials at their particular area — and also, I might add, in several areas by industry people. They have given us quite a good background in some of these technical areas and they're very willing to help us.

At our Command Center, which is located at the Customs Headquarters in Washington, we have a staff of inspectors, patrol officers again, agents and intelligence analysts. The Command Center acts as a clearing house for referrals from the field regarding licensing questions, detentions and seizures. For example, an Exodus team will detain an item because it lacks proper documentation as to whether it needs a validated state or commerce license. The particulars are furnished to the Command Center for transmittal to the concerned agency (i.e., the Commerce or State) for license determination by that agency. Depending upon the decision of the licensing agency, one of three things will happen. 1) It will be released back to the exporter for shipment. 2) It will be seized for administrative action, meaning there was no criminal violation but there was an administrative violation. 3) It will be seized and held for evidence and an investigation will take place, in case there is criminal probability.

The Command Center also develops and analyzes intelligence and disseminates it to the field location and conducts liaison with other concerned agencies. Also, overseas, we have 8 Customs Attache Offices who are located in Ottowa, London, Paris, Rome, Bonn, Tokyo, Mexico City and Hong Kong. We are also opening an office in Soule and we are planning, or have proposed to the State Department offices in Bangkok, Singapore, Athens, Panama and Dehli. And I did not volunteer for Dehli. Depending on the location, much of the work that they are doing overseas is concentrated on export control enforcement, particularly on critical technology diverge. Obviously our offices in Europe are catching the brunt of this, and particularly of course, the office of Bonn. I would say probably 75-80% of their entire case load is on critical tech cases. We also, of course, enforce narcotics laws, currency laws and the fraud laws. But here we have a priority, and our highest priority and our emphasis is being placed on critical tech diversion.

We also developed, through our investigations through other agency information and through our own information, target development. What do we look for? We just don't arbitrarily go out and rip open the first box we come to. We develop profiles for suspect shipments. We look for routings of diversion. We have listings or continually update listings of suspects and suspected shipping methods. For instance, we're not going to concentrate on a shipment of linen going to Venezuela. However, if we get a box that says sewing machine parts to Austria, we're going to open it. We also are interested in computers, like 100 computers going to a South Pacific island. And, believe me, this has happened. Some people just don't think. So we don't just go out there and just look at the 100 boxes and pull out every 5th one. We *do* have a plan of action. Of course, some of the exporters don't think so. But, we do. Our investigations are focused on, of course, violations of the export law. And it is emphasized where these violations occur when the Soviet or Sino block are involved. We have, at any given time, approximately 120 to 150 significant investigations underway involving actual or potential violations of the laws. Several of these investigations are coordinated with other federal or foreign agencies, including the CIA, the FBI, DOD, and overseas customs and police services. I will discuss several of these investigations later on.

First of all, before I give you the results, I have to describe the difference between a detention and a seizure. A detention is an administrative action which is taken until a proper licensing determination can be gained from either Commerce or State. A seizure is a formal legal action and can only be disposed of. Once we seize an item, it can only be disposed of through a formal legal process and goods, in some instances, if the violation is severe enough, can be forfeited to the government. That also includes conveyances that

the goods are being shipped on. Obviously, we don't seize the TWA jet if the goods are being placed on it. However, if it's a private jet, we will. In fact, about a year and a half ago in Houston, you may recall, we seized 1,400 weapons including 1,100 M16's that were being exported illegally. We also seized the conveyance which was a 707 jet airliner. Presently, it's just about out of the courts and it will be forfeited to the government.

Statistics — before I give you statistics I noticed Irv has got his pen ready. Irv, I just want to say that these statistics have a statistical variable of 100%, plus or minus. Detentions from the conception of the program in October of 1981 to date, meaning the last day of May, have been about 2,400. There were detentions where they were called into the Command Center for a licensing question or determination. The seizures in this fiscal year, fiscal 1983, October 1982 to date (again, the last day of May), there have been 860, worth approximately $31,800,000. Since the inception of the program of October '81 to date, about a year and a half worth, have been 1,644 with an approximate value of $89,600,000. They have ranged from everything from soup to nuts, so to speak. But most of these seizures have, or are, technology items (computerware and other electronic aparatus). We did have one shipment that was manifested as bed sheets that somehow got opened and turned out to be bras. We did seize that because it was falsely manifested. I just want to make a point of this because of the fact that you better have your documents in shape.

Investigations — from the inception of the program in October of 1981 to now, we've had accepted for prosecution in various Federal courts, 217. We've had 192 indictments, 222 arrests and 155 convictions. Compare these with figures from about 10 years ago and it's probably about 10-fold. We've increased this area of export and enforcement. Let me cite some of the cases that we've had. Some of them I cannot give you names because some of them are still under investigation. So I'll just have to generally allude to them. The first case is a land resources management case of a company that existed in California. It involves a divergent of state-of-the-art computerized airborne land scanning systems. It's like a mapper that is put in an airplane and it goes over and takes maps. I'm not familiar with the technical part of it but I understand it is quite important. A private corporate jet owned by the company took this equipment from California to Mexico City, completely unlicensed. It required a Department of State license. In Mexico, the documentation was then prepared, that it was meeting the equivalence of Panamanian origin, and was to be shipped to Switzerland and then on to the Soviet Union. We initiated the investigation in response to information from a confidential source that the company would try to export this (it's called a multispectral scanner) and ship it, as I said, to the Soviet Union, via Switzerland. In March of '82, the company did, as I said, via their corporate aircraft, ship a part of the shipment to Mexico City. In Mexico City, the shipment was relabeled by the company and the shipping documents substituted which reflected that the shipment originated in Panama. With the cooperation of Mexican Customs, the U.S. Customs Attache, who was in Mexico City, assured that the shipment was loaded aboard a plane bound for Amsterdam, but flying via Houston. When the plane arrived in Houston it's shipment was taken off and the equipment was removed, and in place we put concrete blocks and sand. The altered shipment was then placed aboard the plane and it went onward to Amsterdam and then ultimately to Switzerland. We cooperated, of course, with local customs authorities in Amsterdam and in France too, because there was a French connection to this, and also with the Swiss police. Presently, there are 2 defendants in this case, and they are both fugitives — both in Europe. In February of 1983, on this one I can't mention names, there were approximately 15 search warrants served at the same time in 3 countries, including the United States, in connection with an investigation regarding the diversion of computer equipment. The customs service of the U.S. and the 2 other countries involved succeeded in destroying a major international organization involving the illegal movement to the Eastern bloc of strategic technology This cooperative effort revealed that these firms and others in each of the countries had moved millions and millions of dollars of sophisticated U.S. and Western technology to the Soviet bloc during the past several years. Through the search warrants and the documents that we gained, there were literally hundreds of shipments that went through this way.

In another case, we had a case of the illegal diversion of bubble memory crystals and wafers. Licensed partial shipments of the total system were exported to a Western European country and then, at that point, they are put together to make the final unit. The equipment when assembled will include all the components of a bubble memory crystal factory. These shipments are being monitored by us, meaning the U.S. Customs and by the authorities of that particular country. When we think we have enough evidence both services, ours and theirs, will move and take these people off.

In late 1980 to September of 1981, Temcom Corporation, a company in Northbrook, Illinois, illegally shipped approximately $16,000,000 worth of C-130 (that's Shinook Helicopter parts) to Lybia in violation of the arms export control act. Temcom concealed the military nature of the parts by stating that a civil aviation corporation was the user. This company, United Africian Airways was in fact acting on behalf of the Lybian Airforce. On September 10, 1981, our office in Chicago detained three shipments which were worth over $1,500,000 million dollars and then shortly thereafter executed search warrants. Presently, one person is a fugitive and the other two have been indicted and are waiting trial and we have, meaning the customer service, formally seized these aircraft parts and now have them where they will be forfeited to the government. In March of 1982, an individual by the name of Cied Cigaria upon his arrival at Dulles airport in Washington was searched and found to have numerous documents reflecting his agreement to illegally sell M60 tank parts to Iran. He planned to utilize false Pakastanian and user certificates and ship the parts to Iran via Pakastan. Pakastan officials refused to supply the certificates and the transaction was never completed. As a result of the search and subsequent investigation the individual plead guilty and was sentenced to one year in prison. This is an example of the elicit transfer of technical data. The final case, which some of you may be aware of, is regarding a guy by the name of Warner Brookhausen. Brookhausen with the aid of middle men in the United States and in other areas has purchased technology items worth several millions of dollars and has shipped them to the Soviet Union. He's now been indicted twice by us, but there's not too much we can do as he resides in Germany. The U.S. Customs in cooperation with German customs in one particular case, were able to delay one sensitive shipment going to Germany, going into East Germany, meaning we delayed it in Germany allowing a second more sensitive shipment to be substituted again with rocks. The German officials in cooperation with us then made a controlled delivery of the item and arrested some violators in Germany. Controlled delivery is where we let it go, but we follow it all the way. It's an investigative technique. Going back to some of the problems we're encountering, first of all, is educating and informing the industry. Before we begin our enforcement actions, meaning close scrutiny of exports. It was almost like an open door. Hardly any inspection or enforcement action ever took place. It was of course a subsequent large loss of technology. The Exodus program is geared to enforcing the law and insuring compliance with the law. We are assisting the industry and showing them how to comply with the law and the regulations. The program is not designed to hamper legitimate trade. As many of our exporters think it is. We're not there to stop you from making money and from letting the material go if the material is properly licensed and documented. I just can not over emphasize particularly you people in industry, when you go back you should tell your export managers to have proper documentation and licensing. Be particularly careful in describing goods and the destination. Don't have your export department send something down to the airport labeled as "computer parts." Because we're not going to let it go. Our customs inspectors don't have the expertise to pick up a box, look at it and say whether it needs a license or not. We've had many many instances in this and you can put it to your freight forter he should know the rules and the reg's. Thats what your paying him for. We had another example where a whole van arrived labeled as "airplane parts". Obviously, we're not going to let it go. We don't know if its military airplane parts, civilian airplane parts, rocket parts, whatever. So, until we get a proper documentation listing and everything else it's going to be detained. Now, probably our biggest complaint is detention time. Customs does not administer the law. We just do the enforcing. Detentions are made by customs, true. But the information is referred to the administrating agency, either Commerce or State for a licensing

determination. We make these referrals almost immediately and in no case more than 24 hours which would include a weekend. So, if you have a problem, if some of your goods are held up, call the particular department where the licensing takes place. You can come through us, the Exodus command center, and we'll refer you to them. Our Exodus command center, incidently for you that want to have the number in Washington, is 202-566-9464. Unlike the lady yesterday who gave out her office number I won't. No seriously my number is 566-5104. We'll give you the commissioner's private number too if you have any complaints. No, we won't. Cooperation between industry and Customs. Again I have to reemphasize, we are not out to hinder your legitimate trade. We are in place to insure the compliance with the law so that our ultimate goal, stopping elicit transfer of technology to our enemies can be achieved and this of course includes the transfer of technical data. Which is probably as big if not a bigger problem than the transfer of the hardware. We of course are having real problems with it as you probably can well imagine. Here I have to emphasize when your corporate executives and engineers are attending conferences overseas make sure that they realize what they're carrying. That's taking out technical documents. Make sure they know the licensing procedures. Because we are stopping not only cargo for examination but we're stopping passengers too and examining them. There's one instance just last week where we stopped an engineer from a company and caused quite a hassle for him til it was straightened out. We wouldn't let him go and we seized the material until it was straightened out later. So, watch particularly your people with security responsibilities. Tell your engineers and your corporate executives about that. We need your assistance also. Insure the compliance or make sure your freight forters know what they're doing. Do they know the laws? Do they know the regulations on exports? Some of them really they don't. You're paying them good money and your goods are getting detained because of their fault and their carelessness and its not fair to you. Make sure your documents are complete and accurate or have you obtained all the necessary licenses? Again, this is a thing that your freight forters should be taking care of. We also need information that you may have concerning real or potential violations. Typical is: Have you been approached or is your company being approached in a suspicious way concerning sales of technology? Believe me they don't come in with the trench coats and the hats, they're very sophisticated. Are you sure of your customer? When he comes in, are you sure that when he says he's going to use this item at a particular firm in Wichita, Kansas, are you sure that's where it's going to go for its ultimate destination? Are there unusual shipping requirements that he levys on you? Does he want it routed via the Mariches Islands in the Indian Ocean? Is it proper business procedure or is there something different or strange? Again like strange destinations, Mariches Islands, or 100 apple computers for 100 people? Sales to unknown companies. Are you sure of the company? If you're not do a Dun & Bradstreet check on it or whatever else your credit department would do. Make sure, I can't emphasize this enough, make sure to whom you sell. Put the profit motivation aside for a minute and think. This thing that you're selling if it ends up in the Eastern Bloc what kind of harm would it really do? In many cases it will do a lot of harm. We have noticed this is one of their main Modus Operandi. The setting up of shell corporations, both here and overseas. They'll walk into a large U.S. manufacturer, hear of critical technology and tell them we'd like to buy your widgit and we plan to have it installed in our factory down the road here. So, the company will sell to them and they'll wish to install it. They will be told, no, no we're sorry we can take care of it ourselves. Oh, Ok and then from there it goes down to this company down the road but immediately it is put on a truck, taken to the airport and shipped out to another shell company in Germany or Austria. Where again it's routed around a little bit and then eventually, there it goes. This goes on and on and on. I can't emphasize it enough to you, know whom your selling to. Are they giving you or do they wish to make unusual financial arrangements in the purchase of the equipment? Do they want to pay you cash? I mean literally cash. Or do they want to give you a cashiers check? Is there something unusual or not a normal financial transaction. Unusual specifications. We had a case about two years ago. A firm in Baltimore called us and said there was an individual wanting to buy a microwave surveillance scanner which is similar to a bearcat scanner except this one scans the microwave spectrum. He assured the firm that it was going to be used

in the United States; however, he told the firm he'd like to have it constructed under unusual specifications maybe 240 volt 50 cycle which is European specifications for electricity. Well obviously the company thought there was something amiss. So, they called us and this is where the industry really helps us. They called us and we sat down with the company and told them good, go ahead take the money, construct the device and then sell it to him and then we'll take it from there. Because we didn't want to hurt the company and that's exactly what we did. It took about four months to build the device. The guy picked it up. We surveilled him when he picked it up in Baltimore and when he got on the plane in New York we arrested him and that was the end of that case. A year and a half later the same company got the same kind of a call for the same device, but a different guy. Again we went through the same drill all over again and this time we learned a little more; however, because it was definitely an attempt by the Eastern Bloc to acquire this equipment and he was going to take it into Germany and then skoot it across the line.

*GOVERNMENT/INDUSTRY PANEL ON INTERNATIONAL TRADE*

**Dean Richardson**
**Manager, International Trade**
**Texas Instruments**

The first subject export control of militarily critical technology will be covered by Bruce Meiser. We will follow that with Art Van Cook talking about the national disclosure policy and then Bruce will again cover how the national disclosure policy impacts the licensing effort. I'd like to just say at the beginning here that we've saved the best for the last and I hope that this panel will prove this. I think that over the past two and a half days this seminar has concerned itself with regulations, restrictions and enforcement. All the things that businessmen look upon as nonproductive in a free enterprise system. It should be evident by now that innovative practitioners in classification management can save their company a lot of money and be much more cost effective and actually turn the cost of security around in the profit and loss sheet. During this panel discussion we're going to discuss government controls that negatively impact business, but we're also going to explain why they exist. How you can carry on your business profitably in such an environment. Nothing happens until somebody sells something. It's an old business axiom which is particularly relevant in our nations current economic situation. The long term health of our economy depends on expanding international markets for our goods and services while keeping domestic sales high. Unfortunately, every industrialized nation in the world has these same pains. Believe me the competition in foreign industry is tough. Immediately following World War II, our productivity far out stripped the rest of the world. Our industries felt no pressure from foreign suppliers. However, over the years our trading partners have modernized their plants where in some areas we haven't. It used to be Boeing vs. Douglas. Now it's Boeing vs. British Air Bus. The battle between GM and Ford is now between GM and Datsun. It used to be GD vs. McDonald now it's GD vs. Dassault. Comparative products overseas are hurting us in the domestic market and are beating us out in many foreign markets. We can no longer have a captive US foreign market. As a result the US balance of payments has flip flopped and we now import more than we export. There was a 38 billion dollar deficit in 1982 and they are predicting a 60 billion trade deficit in 1983. That means we import 60 billion dollars more worth of goods than we export and that's pretty bad. The economists warn us that unless we get a bigger piece of the global market, unemployment will remain a serious problem. The name of the game in the future may be export or die. Today we hope to give you some ideas that will help you and your company manage this awesome challenge.

Our first speaker, Colonel Meiser, for several years has been the DOD munitions control interface between the anxious and sometimes irate contractors and the harried and sometimes intransient military department license reviewing officers and he still looks pretty good, in spite of the guff he has to take from both sides. Probably the biggest challenge facing Colonel Meiser and facing the Department of Defense is boiling down that 700 page secret document known as the Military Critical Technology List, or the MCTL, to a usable document for government and industry. Right now I bet there's not one percent of the companies represented here that have ever even seen or had access to the MCTL. Following Bruce's

discussion our young friend, Art VanCook, the former Chairman of the MVP Committee — with the blessing, I might add, of Britt Snider, DOD — will discuss the MVP and then Bruce will address how the MVP impacts licensing approval. Joe Smaldone will then discuss the ITAR. We will then hear from Dick Williams and Junius Layson regarding making shipments to foreign countries. Our final speaker, talking about visits of foreign customers will be Ed Silver.

So let's lead off with Colonel Meiser addressing the MCTL.

**Colonel Bruce Meiser**
**Office, Under Secretary of Defense,**
**R&D, Department of Defense**

Thank you very much Dean. I'd like to say to all of you that I'm grateful for the opportunity to be here this week. The fact of the matter is, it's a distinct pleasure and honor. Pleasure in the sense that, as Dean somewhat suggested to you, anytime a guy like me can kind of get away from between a rock and a hard place in Washington, D.C., as a Redskin can come out here to Cowboy country — it's a real treat. And beyond that, an honor. Because I did arrive on Monday, I've had the pleasure of hearing the deliberations that have been going on here now for the past 2 plus days. And in-as-much as it's the first opportunity I've had with NCMS, I want each and every one of you present here this morning to know how impressed I am. I think you have just got an *outstanding* society and one that I look forward to having continued relationship with in the days ahead.

I think that Jim Bagley's comments this morning, to put in perspective before you as relates to international affairs, is certainly appropriate as kind of a keynote for something that would be useful to keep in mind in reaching for the 20th anniversary next year. Because, certainly in this growing international marketplace, we find that there is a definite need for communication to take place between us bureaucrats in the Government, and you good people out in industry that are making it all happen. I think the vitality of this particular society is again evident here this morning. I can judge by the turnout that I see. And after your wild and wicked night at Billy Bob's last night, I think that's real "proof in the pudding."

I'd like to make a couple of observations for your benefit and my attempt to put things into perspective, before I get down to wrestling with a topic that Dean has assigned for me to cover here this morning. I'd like to begin by saying that the notion you've heard during the past several days about technology transfer and concerns certainly stands out as a very loud and clear theme — one that we all need to be concerned about, and certainly one for us all to reckon with. It is very apparent from the comments that we've heard about this important area, that there is a distinct need to tighten up on our procedures to include, of course, not just the area of classification, but quite frankly, the area of unclassified as well. Because as you're going to come to find, a great deal of this sophisticated sexy advanced technology that we're all very concerned about in this country, is in fact, not classified. But rather, it's unclassified. And thus, we're presented with a problem of greater proportions I think than might normally be apparent.

As Dean indicated, the main topic of my lead-off picture this morning is a matter of critical technology. I might tell you that to cover this topic I find it to be somewhat of a difficult task in the short time that we have this morning. But I'm going to do my best to move through it rather rapidly and put things in the proper context just so that we'll understand the language. As I pointed out awhile ago, this international marketplace is fast growing. During the past half dozen or so years, we've seen this whole arena mushroom. Now we're to a point where things are absolutely chaotic.

The notion of doing business abroad has brought with it a rather unique characteristic that in affect wants to tap upon our technology. Specifically, the fact that as our weapon systems and defense services and products have become very costly in this day and age, many of your foreign customers are insisting upon offsets in the form of coproduction and in the form of industrial participation and projects having to do with the products that you make and which they buy. That by itself can owe its propulsion of offset into the arena is a concern that we have to deal with.

I think it's also appropriate in talking about trends to point out that during the past couple of years there has been a marked shift in the attitude expressed by the administration in this country that came into office in 1981. An attitude that had gone from that of the prior administration, which you will recall was rather negative, when it came to matters involving the marketing and sale of American products abroad to one that we now have inaugurated by the current administration in 1981 I think this presents a real dichromatic situation for us all to deal with today. We attempt in the government to do what can be done to facilitate your international opportunities while at the same time we're doing what's necessary to guard the family jewels. The challenge, I think, of today is for us all to work together and seek ways to stimulate those opportunities, while at the same time making sure that we do what's necessary to protect advanced technology.

Just a word relative to the office I'm with in DOD will help to establish the framework for you too. It was recently retitled the first of this year to be known as the Director of Military Technology and Munitions Control. Organizationally, it does fall within the Under Secretary of Defense for Research and Engineering. It's been there ever since 1979 when a political power play moved it from the International Security Affairs side of OSD. Regardless of where it's been in the past and where it is today, or where it might be next month, it effectively operates sort of across the spectrum, within the Office of the Secretary of Defense, interfacing with the various elements of OSD in doing this job concerned with military technology and munitions control. One of the key functions of the Office, of course, does involve the matter of reviewing munitions licenses that are referred to the Department by the State Department. A little later this morning you'll hear from Joe Smaldone relative to how we kind of mention the system there across the water, there in Washington.

I do want to say on the onset that we have two basic premises in doing our business concerning export. First is that we deal with each case, specifically on a case by case basis, judging it in terms of its merit. And secondly, in doing that review, we operate on a presumption of approval. That is to say that when you apply for a license we figure that it's because you'd like to have it approved. Since that is our philosophy, and because of the fact that on occasion we find that in the interest of national security it is necessary to deny your request, we have a policy that has been in effect from the department for the last 4 years, since I've been with the office, that affords you a hearing at the time the case is under review, in the event there is going to be negative action taken on that case. I point that out at this time for you to keep in mind during the next presentation by my distinquished colleague, Art Van Cook, on the MVP, because you'll come to find that the so called hearing procedure that we have when we are about to be negative in that department does, in fact, come into play from time to time on issues that concern themselves with international disclosure policy.

I'd like to draw your attention within the government to the fact that there are two principle licensing agencies, State and Commerce. Both departments have the authority to issue export licenses from this country. We in Defense do not have that authority but we do interface with both of those departments with the review of the cases. The different review elements within the Department of Defense are the Air Force, the National Security Agency, the Army, Defense Nuclear Agency, the Navy, Defense Intelligence Agency, Defense Security Assistance Agency, International Security Policy, Joint Chiefs of Staff, National Disclosure Policy Committee, and Office of the Undersecretary of Defense for Research and Engineering where the technical reviews are done within OSD, and of course the International Programs and Technology Office within OUSDR and E.

The mission of our office is simply to establish the department's position on matters concerning munitions license export — those matters that are governed by the ITAR.

The next chart I show you, I'm going to leave there for just a moment because I want to give you an opportunity to look now on both the left and right hand columns. It essentially is a summary, somewhat of a checklist, not necessarily all inclusive but certainly complete enough to indicate to you those key aspects of consideration that we consider in reviewing these applications for export.

Chart 1

# GENERAL CONSIDERATIONS

## PRO–(NEED)

- STRENGTHEN AN ALLY
- FREE WORLD DEFENSE
- SELF DEFENSE
- AID INTERNAL SECURITY
- INCREASE STANDARDIZATION
- OBTAIN U.S. MILITARY RIGHTS
- FOSTER U.S. INFLUENCE
- INDICATE SUPPORT FOR COLLECTIVE MEASURES
- PROMOTE CORDIAL RELATIONS
- *● FOREIGN AVAILABILITY

## CON—(RISK)

- PROMOTE NUCLEAR PROLIFERATION
- INCREASE CHANCE OF HOSTILITIES
- UPSET BALANCE OF POWER
- PROMOTE ARMS RACE
- *● RISK COMPROMISE OF CLASSIFIED U.S. INFORMATION
- *● RISK LOSS OF TECHNOLOGICAL ADVANTAGE
- CREATE EXCESSIVE ECONOMIC BURDEN
- ADD OVERLY SOPHISTICATED WEAPONRY
- ARM A DICTATORSHIP

I would highlight for your benefit, just a couple of areas under Chart 1 notice the bottom left one under the Pro column "Foreign Availability". Something relatively new perhaps, for you to see from the Department of Defense, but one that I want to assure you stands right in the context of the overall review that is given. Because as Jim and others have indicated here this morning, the fact is that we simply must recognize that the competition that you are facing from your competitors abroad is stiff. And we in America are simply not the only producers of the goodies that those customers around the world want to buy.

On the right hand column of Chart 1 a couple of areas that I have highlighted for you, about half way down, happen to be right together — the one having to do with risk of compromise of classified U.S. information of course in the Column category, and right below it — the matter of risking the loss of our technological advantage.

Chart no. 2 briefly summarizes the key significance of the controls as we review them within the Department of Defense from the standpoint

Chart 2

# MILITARY SIGNIFICANCE OF CONTROLS

- OUR SECURITY IS BASED ON DETERRENT STRATEGY
- RESTS ON MARGIN OF MILITARY ADVANTAGE
- MAINTAINING MARGIN INVOLVES HEAVY DEFENSE COSTS
- EFFECTIVE EXPORT CONTROLS HELP MAINTAIN MARGIN

of what you paid us to do in the sense of protecting your national security.

If you take a look at item no. 3 of chart 2 you notice the heavy defense costs that are involved to maintain this necessary margin that we have technologically because of the quantitative

advantage that our adversary faces. The fact is that that hits real hard in the pocketbook. If for no reason other than that, it's terribly important to each and every one of us here in this room. Chart no. 3 that I show you, had to do with the matter of considerations and technology control specifically. Again for the benefit of you seeing how important this is and noting no. 3 particularly, where I mention the controversy involved with the notion of controlling technology as opposed to products.

Chart 3

**BASIC CONSIDERATIONS IN TECHNOLOGY CONTROL**

- **TECHNOLOGY RECOGNIZED AS KEY MILITARY ASSET**
- **NEED TO MAINTAIN A TECHNOLOGICAL LEAD OVER POTENTIAL ADVERSARIES**
- **USE OF CONTROLS ON TECHNOLOGY TRANSFER IS SOMEWHAT CONTROVERSIAL WAY TO MAINTAIN LEAD OVER ADVERSARIES**

I draw your attention at this time, in that regard, to the thing that really kicked off the military critical technology list that Dean referred to in his opening remarks, dating back to the Labuse report of 1976. That is where it was, in fact, determined that the way to proceed was in terms of guarding the technology in a very careful way, while at the same time by controlling the overscrutinizing control of the export of products.

This next chart no. 4 is a simple array or a spectrum to show you how we tend to regard the seriousness of technology transfer ranging from the high to the low spectrum. You'll notice in the high category, for example, manufacturing know-whow. A little lesser importance in the middle category, that of technical assistance. Both of which get into the area of agreements that you undertake with your customers abroad. And then of course, of least importance down in the lower right, those things that have to do with preliminary marketing overtures that your companies wish to make, or appearances that you wish to undertake at trade exhibits.

Chart 4

**TECHNOLOGY TRANSFERS**

| | |
|---|---|
| **HIGH** | **TURN KEY FACTORIES**<br>**JOINT VENTURES**<br>**MANUFACTURING KNOW HOW** |
| **MEDIUM** | **TECHNICAL DATA**<br>**MANUFACTURING TOOLING**<br>**TECHNICAL ASSISTANCE** |
| **LOW** | **PRODUCT SALES**<br>**SALES BROCHURES**<br>**TRADE EXHIBITS** |

Against that backdrop, I'd like to now spend a moment on the matter of the MCTL. As I indicated, the actual beginning of the effort, which has now been underway for some 7 years, dates to 1976. The study that was done under the Defense Science Board following 2 years of study resulted in that so-called Busey Report. I would draw your attention to the fact that throughout the development of the MCTL, there has been active participation by industry advisory groups. This culminated in the Export Administration Act of 1979.

On chart no. 5, I do want to highlight two points. The first that it's the policy to use export controls only after full consideration of the impact on the economy of the United States, and only to the absolute extent necessary. Secondly, to restrict the export of goods and technology which make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States.

Chart no. 6 highlights the composition, you might say, of input to the development of MCTL. Dean had asked me to put this in a perspective for you so you could note that the services all participated. As I pointed out previously there

Chart 5

## MCTL: CONGRESSIONAL MANDATE

"(2) THE SECRETARY OF DEFENSE SHALL BEAR PRIMARY RESPONSIBILITY FOR DEVELOPING A LIST OF MILITARY CRITICAL TECHNOLOGIES. IN DEVELOPING SUCH LIST, PRIMARY EMPHASIS SHALL BE GIVEN TO —

(A) ARRAYS OF DESIGN AND MANUFACTURING KNOW-HOW,

(B) KEYSTONE MANUFACTURING, INSPECTION, AND TEST EQUIPMENT, AND

(C) GOODS ACCOMPANIED BY SOPHISTICATED OPERATION, APPLICATION, AND MAINTENANCE KNOW-HOW

WHICH ARE NOT POSSESSED BY COUNTRIES TO WHICH EXPORTS ARE CONTROLLED UNDER THIS SECTION AND WHICH, IF EXPORTED, WOULD PERMIT A SIGNIFICANT ADVANCE IN A MILITARY SYSTEM OF ANY SUCH COUNTRY.

(3) THE LIST. . . SHALL BE SUFFICIENTLY SPECIFIC TO GUIDE THE DETERMINATION OF ANY OFFICIAL EXERCISING EXPORT LICENSING RESPONSIBILITIES UNDER THIS ACT."

(U) THIS DOCUMENT FURTHER SUPPORTS SECTION 3 OF THE EAA WHICH STATES:

"(2) IT IS THE POLICY OF THE UNITED STATES TO USE EXPORT CONTROLS ONLY AFTER FULL CONSIDERATION OF THE IMPACT ON THE ECONOMY OF THE UNITED STATES AND ONLY TO THE EXTENT NECESSARY. . ."

"(A) . . . TO RESTRICT THE EXPORT OF GOODS AND TECHNOLOGY WHICH WOULD MAKE A SIGNIFICANT CONTRIBUTION TO THE MILITARY POTENTIAL OF ANY OTHER COUNTRY OR COMBINATION OF COUNTRIES WHICH WOULD PROVE DETRIMENTAL TO THE NATIONAL SECURITY OF THE UNITED STATES; . . ."

were industry members that have been active every since the onset in 1974 and continue right on up to the present time. Aside from that, of course, the other agencies in Washington have participated with DOD as well.

Chart 6

## DEVELOPMENT OF MCTL

### COMPOSITION OF TECHNOLOGY WORKING GROUPS

| | | |
|---|---|---|
| CHAIRMAN | —INSTITUTE FOR DEFENSE ANALYSES | —TECHNICAL LEADERSHIP AND ADMIN SUPPORT |
| *SERVICE MEMBERS | —ARMY, NAVY AND AIR FORCE TECHNICAL EXPERTS | —ACCESS TECHNICAL CRITIC. MILITARY IMPORTANCE; ADVERSARY CAPABILITIES |
| *INDUSTRY MEMBERS | —INDUSTRY EXPERTS (SUPPORT OF INDUSTRIAL ASSOCIATIONS) | —ASSESS TECHNICAL CRITIC. ASSESS FOREIGN AVAIL. IDENTIFY TRANSFER MECH. |
| OTHER FEDERAL AGENCIES | —DEPARTMENT OF COMMERCE INTELLIGENCE COMMUNITY DEPARTMENT OF ENERGY | —ASSESS FOREIGN AVAIL.<br>—ASSESS ADVERSARY CAPABIL.<br>—PROVIDE TECHNICAL EXPERTS |

Chart 6

## DEVELOPMENT OF MCTL (CONTINUED)

### DOD CRITICAL TECHNOLOGIES CRITERIA

- POTENTIAL MILITARY BENEFIT TO THE USSR THAT COULD RESULT IF THEIR CAPABILITIES WERE IMPROVED
- DEGREE AND NATURE OF U.S./ALLIED LEAD
- STATE OF ART OF A GIVEN TECHNOLOGY IN THE SOVIET UNION

The subject of chart no. 7 has to do with criteria established for the development of the MCTL. Again I think it is rather self explanatory, given the concerns that you've already heard over the past 2½ days about our technology falling into

Chart 7

## SCOPE AND CONTENT OF MCTL

- **NOT A CONTROL LIST**
- **EXPRESSES DOD ASSESSMENT OF MILITARY CRITICALITY**
- **SUFFICIENTLY DETAILED TO SUPPORT CONTROL LIST REVIEW AND DEVELOPMENT**
- **SUPPORT TIMELY AND CONSISTENT LICENSE REVIEWS**
- **DOCUMENTATION IN-DEPTH**

the hands of the Soviet Union. And that's really what it's all about.

I want to emphasize something, because of a common misimpression about the MCTL. Let me say first, for those of you who haven't seen it, that right now it's in its third revision, having first been published in 1980. It is still classified. The index for it is about the size of the New York City telephone directory. And that's just the index. And you can appreciate, perhaps, from that idea the mammoth nature of this thing. But in point of fact, it is not currently, nor is it intended to ever become an absolute control list. It's purpose instead is to identify the key areas for control and to serve as a guide for reviewers within the government when it comes to the issues that they are assessing for export from the United States. Essentially, it is a reference document, and only that.

Chart no. 8 shows what were perceived to be the principle uses of the MCTL once it is established. In regard to the development of adequate lists, it is intended again here to serve as an aid, nothing more. With regard to the efficiency of a license review process, I would add that of course another spinoff from that will be the improved consistency that should be achieved I think by our mammoth department review in terms of making sure that what happens today is not done in a different way tomorrow or next week.

Chart 8

## USES AND POTENTIAL USES OF MCTL

- **—FOCUSES EXPORT CONTROL PROCESS ON TECHNOLOGIES IN-LIEU-OF COMMODITIES**
- **—DEVELOP ADEQUATE EXPORT CONTROL LISTS**
- **—EFFECTIVE AND EFFICIENT LICENSE REVIEW PROCESS**

The current status of the MCTL, as of this month, is now in it's third revision undergoing review and comment, which is due back in from all the agencies to OSD and our office on the 15th of July this year. And it's anticipated that based on those comments received the middle of next month, there will be a 1983 version scheduled for publication in October of this year.

I would say that this has been the model of the Department of the Defense for a number of years and will continue to be that model for years to come. As I said before, we need to work together with you in industry to find ways that we can facilitate your opportunities to do your thing internationally abroad, while at the same time maintaining the necessary control over those things that would be important to the future health of this country.

I want to thank you very much for your attention this morning.

**Art Van Cook**
**AVANCO International**

Good Mcrning. I've been asked to talk by Britt Snyder, who by the way regrets that he could not stay for the duration of the seminar. But as he explained to you, there was pressing business back in Washington. But he did ask that I convey to you his regrets and that I outline for you some of the salient features of our National Disclosure Policy.

First, let me say that the National Disclosure Policy, which governs the release or disclosure of classified military information has been examined and reexamined over many years. And if you take any policy that specifically provides for exemptions to policy, you have introduced into

that policy, flexibility. So it has been found by many studies that the National Disclosure Policy is flexible — that is in keeping with our current situation. And that it can be applied in a practical way to individual cases that arise. It is the policy of the United States Government to treat classified military information as a national security asset that must be conserved and protected. And that may be disclosed through foreign governments and international organizations only when there is a clearly defined advantage to the United States. In recognition that it may be to our national interest to share classified military information and material with our NATO allies and other friendly nations, the National Security Council, with the approval of the President, issued a national security decision memorandum that promulgates a policy applicable to the disclosure of classified military information. The basic authority governing the disclosure of U.S. classified information is set forth in this national security decision memorandum. That document assigns responsibility for the control of classified military information jointly to the Secretaries of State and Defense and prescribes that they consult with the Director of Central Intelligence, the Secretary of Energy and other agency heads and the Executive Branch as appropriate. Further, this national security decision memorandum charges the Secretaries with the responsibilities for the establishment of an interagency mechanism and procedures to implement the disclosure policy. It charges them to promulgate specific disclosure criteria and limitations and the submission of an annual report for the National Security Council on disclosure activities, and finally the review of intelligence, the conduct of on-site security surveys and a negotiation of general security of information agreements (GSOIAs) to determine foreign recipients capability and intent to protect U.S. classified military information. Now we have in place, or being negotiated, some 40 general security of information agreements.

The interagency document which implements the national security decision memorandum is entitled national policy and procedures for the disclosure of classified military information to foreign governments and international organizations. And briefly it is known as NDP1. This implementing document is issued by the Secretary of Defense with the concurrence of the Secretary of the State, the Director of Central Intelligence and the Secretary of Energy. The basic policy does not pertain to the control of national intelligence and counterintelligence. The responsibility for foreign disclosure of that information is vested in the Director of Central Intelligence. The policy does not cover communication security, equipment or information. That responsibility is vested in the United States Communications Security Committee. It does not cover atomic information which is controlled by the Atomic Energy Act of 1954 as amended and it does not pertain or govern the foreign disclosure of special compartmented information which is the responsibility of the Director of the National Security Agency and the Director of Central Intelligence. It does not govern the disclosure of strategic planning and guidance which is the responsibility of the Secretary of the Defense and the Joint Chief of Staff. So you have a policy here which governs many things, but does exclude some and when you have a policy that has this type of exclusion in it, there are some difficulties in implementation. I think many of the problems, that come up are for access by firms doing business in the United States under foreign ownership control and influence of a foreign firm.

The National Disclosure Document sets forth specific criteria and conditions which must be satisfied before a decision is made to release classified military information to foreign governments and international organizations. Now these criteria are practical and I would expect the same criteria that governs the release of foreign information to the United States. I was told by Edgar Hill of the UK that our National Disclosure Policy pretty much parallels the National Disclosure Policy of the UK. The disclosure criteria is that the disclosure is consistent with the foreign policy of the United States toward the recipient nation or international organization. Secondly, that the military security of the United States permits disclosure. Third, that the foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States. Next that the disclosure will result in benefits to the United States at least equivalent to the value of the information disclosed. And lastly, that the disclosure is limited to information necessary to the purpose for which the disclosure is made. That last one is briefly that we are asked

by a foreign government the time. We don't tell them how to make the watch. We give them the time. For all of the countries with whom we exchange classified military information throughout the world, we have established in the implementing document, levels of eligibility for certain categories of information governed by the National Disclosure Policy. This is guidance. There are exceptions to these levels. If the department of the Army, for example, needs to release classified information to a foreign government which exceeds the eligibility levels prescribed by the implementing National Disclosure Policy document that would involve an exception to policy. If the Department of the Army or the Department of the Navy or Air Force needs to disclose to a foreign government information that does not meet all of the disclosure criteria that involves an exception to policy. These requests for exception to policy are referred to the National Disclosure Policy committee. The committee is comprised of six general members. Representatives of the Secretary of Defense, who also chairs the committee, representives of the Secretary of State, representatives of the Secretaries of the Army, Navy and Air Force and the chairman of the Joint Chiefs. Those general members have an interest in all matters brought before the committee. There are also special members on the committee representing the Director of Central Intelligence, the Director of the Department of Defense, Defense Intelligence Agency, the Office of the Secretary for Research and Engineering and the office of the Secretary of Energy and other offices in the OSD. During calendar year 1982 this committee handled a total of 134 cases. Of these 110 involved decisions on exceptions of policy made by the committee. Seven called for decisions by the Secretary of Defense and the remaining 17 involved decisions on amendments to exceptions to policy already made. In the workings of the National Disclosure Policy committee when there is unanimous agreement between members on a decision to release classified military information to a foreign government, that is an easy one to handle. Thats a go and no go. Unanimous Agreement. If there is a split vote in the committee the chairman must issue a memorandum announcing his intent, after weighing the positions of the members, to decide the case one way or another. Deny or approve. The disenting members have the right to appeal that proposed decision to the Secretary of Defense within 10 working days. That decision is final. If there is no appeal made to the Secretary, the chairman's decision remains as a NDPC position. Each year there are about 12,000 disclosure decisions made and the committee of course cannot handle this volume so the authority to make a disclosure decision is delegated to the secretaries of the military departments, the Under Secretary for Defense of Policy, the Under Secretary of Defense for Research and Engineering and to the Joint Chiefs of Staff. They in turn are authorized to re-delegate that authority in writing to whatever levels they feel appropriate in their respective organizations. The head of the Naval Material Command for example, may be given disclosure authority in writing by the Secretary of the Navy. That disclosure authority is limited to the information over which that individual exercises jurisdiction. Disclosure authority given to an individual in the Navy cannot be exercised over Army information or Air Force information. This then is the salient features of the National Disclosure Policy. I just want to summarize by saying that it is a policy that is flexible. The committee is a dynamic one. It is one with specific authority to act on every case brought before it and the turn around on cases that involve exceptions to policy is 10 working days under normal circumstances. I just want to mention that the policy that I outlined for you here is very much kin to the policy of other countries with whom we exchange classified information. It is in the implementation of these polices that we come to the problems that were eluded to by my distinguished colleague Mr. Jim Bagley I think we share the same problems whether its here or there and we have to find solutions to them.

**Joe Smaldone**
**Office of Munitions Control**

The Arms Export Control Act is the statutory authority under which munitions that is military type equipment, is subject to export control. The Arms Export Control Act authorizes the President to designate or identify those items that are subject to control and to develop the necessary regulations for carrying it out. Now of course the President doesn't do any of this business, its guys like us at this table who do it all in the name of the President. What we have done is come up with something called the ITAR (International

Traffic and Arms Regulations) which are the body of regulations governing the export of military equipment and associated technical data. I was supposed to say something about the update of the ITAR. When I came into the Office of Munitions Control three years ago there was then in preparation and we published in December of 1980 a proposed revision to the regulations. I am happy to say three years later things are still where they were. We got about 3 volumes of comments from that publication. We have looked at them all, digested them, thought about them, redrafted and rewritten them. Its been up and down and I just don't see when the immediate future is going to bring about another addition for public comment. Every time we seem to be making some progress our legal advisor for whom we depend a great deal to do the fine tuning on this winds up being detailed off on more pressing matters and like everything else the ITAR is not the most significant item when there are wars being fought around the world and base rights to be negotiated and things like that. In any event I don't think anyone ought to worry about it. Whatever does come out will not be a profound revision or change. There will be some changes to be sure but in the meanwhile we just continue to march under the current regulation. Well what the ITAR does is to identify in the first part, so called munitions list, which is the list of equipment subject to export control and also technical data that pertains to such equipment. They are equally subject to the licensing requirement. The Office of Munitions Control in the Department of State is responsible for administering the licensing process and that covers both classified equipment and technical data as well as unclassified. We don't make distinctions in our licensing process between the two. As far as we are concerned the regulations apply across the board. Those of you here are probably principally interested in classified equipment but I have heard so much over the last couple of days on unclassified but sensitive technology to make me think you would like to know that our authority and our activities do cover the entire spectrum. We got about 40,000 cases last year requesting approvals under licenses or other type of authority for exports of equipment and technical data. That is a rather large case load and it has been increasing steadily over the years at about a 10% compounded rate. Of that number, only about 1,000 are for classified exports so you can see as far as we are concerned the classified portion is relatively small. Virtually all of these licenses for export of classified military information or equipment are refered esentially to Bruce Meiser's office and to the appropriate other DOD agencies for review. They are responsible for reviewing and providing us with recommendations whether or not this export should be permitted. In that process of review with Bruce that Art Van Cook had mentioned the National Disclosure Policy comes into play and the license application will be reviewed to determine whether or not it is permitted under current eligibility levels for the proposed country of destination or whether an exception to policy is required. If so the Department of Defense or occasionally the Department of State would be willing to sponsor an exception to policy. If that is not the case then the license will be denied because it fails to satisfy the NDP criteria that Art has explained.

I would like to focus my discussion this morning principally on technical data exports because I think that is where most of the concerns and problems arise. I would like to again emphasize that the technical data controls that I am discussing apply exclusively to that which relate to articles on the munitions list for which we do not have any authority. We do not have any business in technical data that relates to items subject to Department of Commerces export control. If you can keep that exclusively aside for the moment I would like to bring us back on the munitions track with regard to the definition of an export for technical data. We regard any kind of disclosure either oral, visual or documentary of technical data outside the country or to any foreign national inside the country as an export. In other words, you do not have to leave the shores of the United States to complete an export transaction. If a foreign national visits your facility or approaches you at a technical gathering and technical data is disclosed to that person and if such technical data would require a license if sent to that person or disclosed to that person abroad then a license is required for that in the United States. The site of the transaction is immaterial. The process that is regulated is the export and that can take place again by oral, visual or documentary means. For classified disclosures the matters are rather simplified by the existance of industrial security procedures and regulations and the good working

relationships between the Department of Defense and contractors in that respect because the regulations are also elaborate and precise. The likelihood of problems arising in that arena are relatively small compared to the unclassified side but I would say that again referring back to the fact that we do issue about 1,000 licenses a year for classified disclosures for either equipment or technical data that there are in our regulations both exemptions and requirements for licenses and I'll mention one of the exemptions simply to make it clear that we don't duplicate effort. If there is a foreign visit to your facility during which classified information will be disclosed, if that visit is pursuant to a defense approved plant visit then a state department license is not necessary. We don't want to duplicate the work of the Department of Defense in that case. However, if the Department of Defense does not sponsor or approve or is not otherwise involved in the visit of a foreign national to your organization and in the course of that visit classified information is to be disclosed then an export license is needed because in that case we have a direct transfer of information from the U.S. party, i.e. the contractor to the foreign national without the Department of Defenses approval by the plant visit routine. So in effect it is a direct transfer. There is no U.S. Government involved in it. The U.S. Government becomes involved through the licensing process. An unclassified disclosure that is made to foreign visitors in connection with a DOD approved plant visit does not require a license. If you have a classified plant visit most likely there will also be unclassified information disclosed along with the classified. That is covered specifically by an exemption in the regulations. You don't need to get a separate license to cover the unclassified if you have authorization under the plant visit to cover the classified. On the other hand, the visit or if your discussions with foreign nationals are strictly at the unclassified level they do require a license because normally the Department of Defense does not sponsor unclassified visits of this type. Again the classified is generally well covered and established for the regulation. On the other hand, unclassified visits generally have a marketing nature or exploratory discussions. If tech data is to be disclosed then you should provide for an appropriate license.

Having said that as an introduction let me speak briefly about four special interest topics. One is the nature of the U.S. Munitions list. I wish to emphasize that the munitions list is essentially a joint document. While it is part of the Department of State Regulations the content of that list is determined jointly by the Departments of State and Defense. Neither one of us can unilaterally add to or subtract from it. An item is not considered to be on the list unless there is agreement by both agencies. There are legal as well as practical considerations. We need, obviously, before determining that we can put something on the munitions list, to assure that we have the legal authority to do so. We also have to consider the enforceablility of that determination if we decide to put something on the munitions list. That involves everything from licensing kind of enforcement to the kind of thing which Meed Fields spoke to you about, where, this has to be enforced at the working level, not the level of the company rep who is doing travel and things of this nature.

The second item I wish to mention is that of employment of foreign nationals, or the use of foreign nationals as consultants by companies and defense contractors. You remember earlier, I defined an export and also indicated that an export is considered to take place anywhere whenever a transfer or disclosure of technical data is made to a foreign national, regardless of the site. We know and have discovered that there are many foreign nationals working in U.S. companies. We know that foreign nationals are employed as consultants occasionally, on various projects — strictly at the "unclassified" level. Then again, I'm not worried about the classified because I think the Industrial Security Procedures are quite adequate. But on the "unclassified" side there was a misunderstanding that existed, I think, in certain quarters, to the effect that, well, since you employ someone in the United States — even though they're foreigners and even though there is technical data involved in their work — that because there was not a delivery abroad of the information that an export had not occurred. Well, about a year ago, we published in a newsletter a clarification on that matter, and made it quite clear that any disclosure of technical data to a foreign national in the United States, if such data would require a license to be exported abroad, must therefore be licensed in the U.S. So, here

once that happened, we did get a flury of inquiries, letters and whatnot. And we've since been handling this, I think, rather effectively. Where companies do have foreign nationals, they have simply been consulting with us about the appropriate means for licensing them. And, we have been doing so under our normal DSB5 Unclassified Technical Data License, rather a more arduous procedure of having a technical assistance agreement. The problem is not as big as it appeared to be initially. Nonetheless, I do want to increase your awareness of the matter. You know, those of you in the security field, particularly if you do have foreign nationals at work in your organizations. I would like to distinquish a foreign national from the immigrant alien. The immigrant alien is a permanently resident, person of foreign origin. In other words, I don't know what the visa's say particularly, but they have been granted a permanent residency status by the Immigration and Naturalization Service. We treat those permanent residents as U.S. citizens as far as our regulations go. It is only those who are here on some kind of a temporary basis that require a license.

A third matter has to do with the problem, when a U.S. Company comes under foreign ownership control or influence. The industrial security procedures, of course apply on the classified side. On the unclassified side, if a foreign company buys out a U.S. Company, I want to emphasize that our authority extends only to regulating exports. Mere ownership does not constitute any change in the status of that company. We do not license ownership, we license exports. However, if that ownership is going to result in the disclosure, ie: the export, of technical data to foreign nationals by being sent abroad, obviously that requires a license. Also if the officers or technical personnel of the parent company, are going to come to the United States to participate in technical activities, to review programs, or whatever, and technical data will be disclosed in the course of those activities, then the license must be obtained. Depending on the circumstances it will either require a regular export license or a technical assistance agreement if it is a long term, continuous kind of arrangement. The two key points here are: Number 1 — Mere ownership or change in ownership, does not in itself change the status of the U.S. Company, with regard to the application of the ITAR. The other point is, if that change in status will in fact lead to disclosures or exports of tech data, then by all means obtain the appropriate license. The fourth point is really the second broad issue that I was supposed to address this morning, and that is expediting export licenses. I will not say all that much, because a number of points have already been made to the importance of being precise and detailed in your attention to filling out licenses, indicating the full details on shippers export declarations and whatever. It does make it much easier obviously, for us to review and process a license if it is very clear what is being done and if the number of copies are accurate. Also if the titles of documents are correct, the description of the equipment is appropriate, and the end users are clearly identified. There is one little block on our export license which asks you to provide the name and telephone number of a U.S. Government Official, who might be familiar with this particular program. That's helpful to us, because it's a clue that if we need to have the licenses reviewed outside of our office. Often there's nothing put there, which doesn't help us and doesn't help you. Often times there's the name of someone in my office who's name is there, that doesn't help either. In fact, it specifically says, do not put the name of someone in the Office of Munitions Control there. I don't take personal offense at this, but I do wonder how somebody keeps an eye on these things when I see the name of my predecessor appearing in that block, who's been retired four (4) years now. Someone's not doing their homework and I can only ask you to do your homework and that will help us to do ours. The other specific question Dean mentioned earlier, that there is some sort of good news on the horizon. He wrote me a letter prior to this occasion where he indicated a couple of cases where Texas Instrument had incurred some incredible lost time, in a sense, in getting an export license. Our practice is to send the original of that license, when approved, directly to the Cognizant Defense Investigative Service (DIS), and it goes directly to the regional Defense Investigative Office for transmission to the appropriate U.S. Rep. That takes time. Dean pointed out a couple of cases, where there was a loss of two (2) or three (3) weeks in this process, from the time we issued the license till it got to the point where it was needed. In the case where there was competition

for an international contract, and bids and proposals are prepared and submitted. That's a very costly loss of time. Now I don't know why it is, but I can only tell you the practice has been that we mail the original license to DIS and we provide to the contractor a copy of the license, so they would know the licenses had been issued and sent. They have their copy in their warm hands and feel good that the license had been issued, and they run back home waiting for the original to show up. The original is the authority which DIS will use to process the documents or the equipment for export. It doesn't show up for two or three weeks. Well you can imagine the problems that arise. Now I have inquired around the office, and I can't find any good reason why we have this practice. It has simply been done and maybe it's a hold over from a previous understanding or agreement. I don't have any real problem in doing it any other way. We permit companies to pick-up all other licenses that are the originals, and if it would be easier for contractors to pick-up the original of the license and to get it by whatever means, to their U.S. Rep. quicker than the U.S. Mail Service, that's fine by us. I don't know how we are going to work this because if we decide to do it this way, we should put a notice in one of our newsletters announcing that: "Henceforth, we will do it." Unfortunately, I don't know when newsletters are going to be coming out, and as a practical matter the person who had done those newsletters has left the office and no replacement is in sight. There has not been a newsletter in a few months, and I don't know when there will be. In any event, at some point in the future, whenever our newsletter comes out, don't be suprised if you find an item in there saying, we now will treat classified licenses, just like any other licenses, with regard to the possibility of your picking it up, for transmission directly back home, as apposed to waiting for it to arrive through the U.S. Postal Service, however it gets there. I think Dean's example was an extreme one. I suspect most of them are not as bad, but in any event, as far as we are concerned, if it will expedite your business, and if you feel better having the original one and you want to be responsible for transmitting it to the Cognizant Defense Investigative Service.

**RICHARD WILLIAMS**
**Chief, Industrial Security Programs**
**Defense Investigative Service**

Let's talk about the DSP85's. First of all, I would like to point out, that there is a circular letter from Joe's office, it's dated November 1979, and basically it lays out all the licenses. It says at the bottom of this letter, "Additional copies of this letter are available from this office, please ask condition control licensing officers for assistance." What I want to point out to you here is that, there is a summary available of all the different types of licenses with specific examples. This would be very useful to you. I would certainly encourage you to obtain a copy, and to use it. It goes through all the different types of licenses that are available. Just because it's not a classified license and it doesn't fall under DIS authority for processing and working with you on Government to Government channel establishment, does not mean that you don't need it, for unclassified exports.

I want to address the problem about the long delays on DSP85's. I just can't sit there and note that takes us four (4) months to get a license out. I went and did some analysis with Lloyd Kelly to try to find out why Dean Richardson can't get a license processed to him in less than three (3) to four (4) weeks. I found out that in November, of 1982 we recognized that we had a problem, in that we were waiting till we had the entire Government to Government channel established before we would release the license. In other words, the State would send it to us and we would hold it. We don't hold it anymore. What we are doing now, is processing them on immediately. Dean, do you feel better? Does that make you feel better? I went through and averaged these out, because I like statistics, and it came out six point seven five (6.75) days which is the current average on the twenty (20) licenses you've had since November of 1982. At any rate, that's the current average, from the time that Joe sends it to the time that we dispatch it to the U.S. Rep.We have no policy that will prohibit a contractor who has a real urgent situation, if State will permit it, from picking up that license from State, and carring it to the U.S. Rep. Now we have two (2) requirments; the first of these requirements is that the

U.S. Rep. must have custody of the original license. You can understand that, because you don't ship everything at one time, especially when it's hardware, sometimes you ship it in increments, even though it's allowed as a total number, you ship it in increments, so therefore, we've got to be able to annotate that and keep up with it. The second thing is, that we've got to be able to physically check the items against the license. Now we have those requirements, and I can't lift those at all, but as far as helping you process them fast, we're certainly going to do that. I'll leave a copy of this license application, which describes all the licenses.

I would like to talk a little bit about Government to Government transmission. Basically, this is an area that is misunderstood. Essentially there are two ways to have a Government to Government transmission. Not one but two. Most people are only familiar with one. And that is to do it in the U.S. Believe it or not, I understand they do it in other parts of the world besides just in the U.S. And in the U.S., we usually have the shipments, however, we can also have them overseas. This is something that is based on two primary policy considerations that we have in DOD, and I would like to briefly mention those two policy considerations. The first one is the international agreements themselves called bilateral security agreements, and also called General Security of Military Information agreements. There are twenty-eight active agreements, signed and in place, and twelve in process, which brings the total to forty. An addendum to those agreements, is an industrial security agreement. There are eleven of those. We also have recipical agreements with the Netherlands, Denmark, UK, Canada, and FRG. Those specifically spell out things that are supposed to happen theoritically. Mr. Bagley did you hear me on that, theoritically. Theoritically, is special considerations in relation to recipical clearances. I would like to point out that all those agreements are not unclassified, and this has caused a problem. This means that when you come to us and you are going to export to a country, you don't know whether or not a Government to Government channel is required, because, we haven't told you what countries we have agreements with. Now one of the things I'm going to do, as a promise to you, when we go back to the office, is to have a list developed of these countries and send them to our Cognizant Security Offices. You should call and ask us if a Government to Government channel is required. A Government to Government channel will indicate we are going to have an agreement with that particular country. Basically, the general security of information agreements have specific things in them. They are all common in that they have some of the same items, although there are some individual differences. There is equal protection of classified information on the part of both countries, the use for specified purposes, to honor propriatary rights and third country release is prohibited. In other words, we don't want to release our information to one country and have it turned around and released to an adversary. This is one area where we get a lot of heat on, and that is why we require Government to Government channels? We abide by the Government to Government channels, because they are part of the basic agreement. Also compromises are reported to the releasing Government. It's very embarrassing, to have compromises and have to report them to the releasing Government. I'll give you an example of one that made me sick to have to report, and I won't give you the countries. We had a Government Rep. that mailed a package to the wrong Embassy and said in the cover letter that it was for another country. It is very embarrassing to have to go over and explain, that we mismailed the thing to the wrong Embassy. Unfortunately, in that case, it went to the Military Attache and I don't have to tell you what happened to the information. The last thing is that there are mutual security surveys. This is something where they come to us and look at our system. We just had this happen here not too long ago. We have people from Switzerland coming to see us in the next week. Let's look at the second policy consideration, NDP-1 simply gives the way we implement the disclosure policy objectives and it mentions specific things about each country. Now let's look again at the Government to Government channels. If a transfer of information will take place in a foreign country, the material must go by approved channels and be accompanied by a U.S. Civil Service employee, or Military person, who is properly cleared and is designated by the contracting officer. The first possible alternative on a channel out of the country is by registered mail, through an army or fleet post office channel. That

means, you have to know who the U.S. Government Representative is in the foreign country. That has been a problem for a number of you, and to solve that problem we have now put out a comprehensive list. I'd like to say we had that a long time, but I just signed it out on the 17th of June. The different MAAGS and personnel in foreign countries are listed and we made that available to Cognizant Security Offices. You can contact your Cognizant Security Office and they can give you the listing. If you plan ahead of time, you'll find yourself not in a bind at the last minute. I'm going to skip over and go directly to the In Country Requirements. Specifically what we have here is that information will be sent to an Embassy and signed for at a U.S. facility by a foreign representative, or sent to an official address of the recipient Government which has extra territorial status. The material also could be sent for loading aboard a carrier designated by the foreign Government at a point of departure from the U.S. An authorized U.S. Representative must be present to ensure secure loading and assume security responsibility for the classified material or the material will be transferred to a cleared U.S. contractor storage facility freight forwarder, or will be sent to a freight forwarder owned or controlled by the recipient foreign Government. Each kind observes Government to Government channels and the transfer takes place in the U.S. This is for temporary storage when the carrier designated by the recipient foreign Government is not available for storage, these freight forwarders must meet U.S. DOD physical security requirements for storage. I might mention to those of you that use the agencies, that's an information security program regulation. In summary, we have two (2) basic requirements: (1) the release is either inside the United States, or (2) outside the United States, where we will work with you to help expedite this. Please contact us if you want to do it outside the United States and we will help give you names of people who can help us establish the channels. Thank you very much.

**Junius C Layson**
**The Boeing Company**

When Dean called me, he said, "I want you to give this and show them how they can do it without tears." I don't know where he's been working, but I've had a lot of tears with it. One of the many lessons that we learn is, you must start planning well before program award. You have to identify what the program schedules are, what your security requirements are, and the various requirements of the Military and Government departments. You're going to have disclosure approval problems. You are going to have document equipment release procedures and communication, transmission, visit procedures. You may have resident foreign nationals and foreign country facility clearances. I'm only going to briefly touch on disclosure approval, and cover transmission procedures.

You must identify your problem areas requiring resolution as immediately as possible. You also have to identify the various Government Agencies having jurisdictions you are going to have to work with. You better plan for extensive time to work the problems that the U.S. Government Agencies, and you are probably going to have to coordinate with foreign Governments. What ever you do, document all your requirements thoroughly. Prepare detailed procedures for your employees to implement, because they're going to be very complex. Two (2) examples that I want to give you that explain the complexity of what you can get into, are the NATO E3A Coproduction program, and a French E3A demonstration. With the NATO E3A program, (this the coproduction program, involving both U.S. and foreign contractors), they would require access to NATO and U.S. classified information, there would be production effort in the United States, and in Europe. There's going to be a large volume of classified data and hardware exported from the U.S. to Europe. And, we are going to have to have expedited movement to meet our contract schedules. And we are going to have to comply with not only the U.S., but the NATO and the FRG security requirements. The major problem areas that we identified, was expeditious export license processing, the expeditious movement of classified material, which was data, hardware that's both classified and COMSEC. We will have problems getting through airport security and custom checks, both in U.S. and Europe. We would have Government to Government transfer point location problems. To give you an idea of the complexity of the agencies that we would have to coordinate with, these are some the principal U.S. Government Agencies involved; I'm not going to

explain what all they are, but I just want to show you, just to give you an idea. We also have the considerable foreign or international pact organization involvement, as you can see from this. We have hundreds of subcontractors involved in the E3A program, but principally, there are thirteen U.S. and seven German contractors who would be involved in classified information or hardware, and U.S. or NATO secret information. At this point and time, before I go farther, I would just like to mention, all the agencies that we coordinated with, we've had outstanding assistance and cooperation. This goes down through Munitions Control with all their staff, and licensing officers, the various department of defense agencies and the like. I'm going to mention a few names through the industrial security channel, because they were the principal ones that assisted us in the transfer of material. And over in OUSD, at that time, Tom O'brien was over there, Art Van Cook helped us, Chuck Wilson, Maynard Anderson, John Freel, and at DIS when Tom went over there again, him, Dick Williams, Joe Sidle, Frank Larson, our regional office Fran Mullin, in Dayton we had John Brickley, down in the Airforce Cryptologic Depot, we had Bill Manley. I mentioned these people, because they spent endless hours. What you will see wouldn't be possible without them. With OMC, because this is a dynamic program, and it would be continual changes throughout, the normal process of giving an export license thirty (30) to sixty (60) days just wouldn't work. The procedures that were established were possible, because the foreign disclosure policy had already been established. The multitude of staff that is required for export license was eliminated in this instance. An agreement was worked out where a foreign disclosure policy officer would be established in our plant. He would work directly with Munitions control verifying that the material that we were going to release had been approved and is within the licenses requirements. It was also a delegation to the AFPRO to approve the release of unclassified information. The treasury and OMC work together for State and decided that the principal monitoring both import and export, because this would be going back, would be handled through department of State. It also worked out where, the export licenses for our sub-contractors could be keyed to our prime contractor export license and there could be a method of identifying through customs and postal to expedite the processing. We eliminated freight forwarders completely. As a result of this, you see that we had an expedited process that not only took care of what I just explained, but through the program offices, where everything is delegated down to the foreign disclosure policy officer, and AFPRO located in our facilities.

In looking at the movement of material, we looked at the various methods. We found none of them were satisfactory. They wouldn't meet our time lines or the weight restrictions, and so on. I'll give you a typical illustration. The only significant thing is you see the flow time extends as much as 27 or 28 days, in many instances, and getting material through by whatever channel you're using. We obviously couldn't live with that. As a result of working with these various agencies, we were able to get agreement that contracted personnel could be authorized to be designated as U.S. Government couriers for hand carrying material across international borders. We had to work with the participating NATO commercial passenger aircraft and got approval to utilize them in lieu of flight carriers only. We made arrangements with these various U.S. and foreign commercial airlines to merit constant courier surveillance of our classified shipments. I might mention that when you are moving any large shipment always use two couriers. You will find that one has to wonder off somewhere to do some coordinating function and the shipment has to be under constant surveillance at all times. Various arrangements were made with foreign governments for exemption from customs inspection at airport entry points. We made arrangements with U.S. and foreign governments for central Government to Government transfer of material to expedite it. We obtained modified NATO FRG COMSEC transmission channel accounting procedures and we expanded the insertion points in the defense transportation system to include subcontractor locations. We received formal written approval for the appointment of couriers and attached to that letter are very detailed procedures of the requirements to assure the classified information is properly protected. As a result of this coordination, whether we are being designated as a NATO courier or U.S. Government courier, we were able to cut the time the individual left our plant to when he got

the material over there to 4 to 8 days. In addition we found that there is a safety regulation which permits under certain conditions material to go through the foreign government customs, exempt from examination. I won't go into great detail, however, I will show you a couple of forms that are involved in the thing. Those regulations provide all the details of how you accomplish this. We submit the form to our designated government representative and identified to him that we are going to make a shipment and that we need an exemption certificate. He issues this exemption certificate and it's given to the foreign customs concern for processing through. This is the one he actually gives to them. As a result of that, our courier leaves our facility and he has expedited processing through the airport in the United States and he has expedited processing through the foreign government airport. He has transmitted to the location. Simultaneously we arranged the U.S. government rep, the FRG rep to the contractor rep all accomplished this transfer in one action. They make a simultaneous inventory and depending on the amount of material we have a complete transaction done in half hour to an hour.

Working with our friends, actually they did it all for us, in both Dayton and the Airforce Cryptologic Depot. As a result of their action, the material actually goes from the depot direct in the NDA in Germany, down to the contractor.

The French demonstration is an example where there is a temporary export. The major problem areas that we found there is the E-3A was going to be in our contractor custody all the time during the demonstration. And of course it contained classified information. We would have a storage problem with the U.S. classified information in France because the test would be conducted at the French airport installation and we had no U.S. installation in the facility or in the vacinity. We had government to government transfer problems because we were going to be transmitting in encripted transmissions from the airplane to the ground and back and forth. We would have temporary exchange of material at the ground test site. We would also have permanent transfer. So we went back to our friends in DIS and as a result we were able to get a waiver of paragraph 17 and paragraph 94 which waived the requirement for us to store the classified material on a U.S. government installation and waived the requirement for formal government to government transfer. This was possible because the U.S. and France had executed a General Security of Information agreement in which they are bound to protect our information. Therefore it authorized disclosure of the information so that we had no disclosure problem. We worked a security agreement with the government of France, with headquarters DIS, and Airforce approval where we incorporated into the agreement the various requirements which would assure the U.S. classified information was being properly protected. Basically this agreement provided for the government of France to designate a security representative with us on all various matters. They would identify those people who needed access, they would provide military guards and physical security measures for our aircraft, they would protect U.S. classified information in our custody for GSOIA. We would establish a joint accountability record and receiving system for U.S. and French information that was being temporarily exchanged, permanently transferred and encripted transmission. They would provide COMSEC key material for secure transmission between the air and ground. Of course they would report any loss immediately and they provide any additional support that we needed. We in turn would also have a designated security rep they would work with. We would control access to the E3A during work periods. We would lock it and maintain surveillance during non work periods. We would identify our personnel that would require access to their secure areas on their air base ground stations and the like. We would protect their French information for GSOA. We would in turn establish accountability records for this information being passed back and forth and if we lost any of their material we would report it immediately. We would also request whatever additional security we needed on site.

In summary, you must immediately identify the problem areas where you are going to have to have resolution. You must identify the problem in detail including the government agency having jurisdiction. They will be able to work the problem for you as well as you identify it. You have to make sure you are giving them the proper information. Don't only come to them bitching about your problem, see if you can't provide a

recommended solution to them and solutions provide the same or better security than are currently required. We have found that all of these government agencies will assist you in any way possible to find an acceptable solution to the problem but you are going to have a long time in working these complex problems. Nothing is impossible, it just takes a little more time.

NOTE: Please see charts regarding this process at the end of this panel discussion.

**Edward Silver**
**Hughes Aiscraft**

Before we start let me make three comments. The first one is that when industry supported DOD on the military critical technology the agreement was that the control was to prevent the loss to the Soviet Union. I would like to emphasize that each time we talk about the military critical technology list it seems to be interpreted to other countries. The second comment I would like to make is that on DSP85's if you follow the suggestion of using a foreign point of release you better get a separate DSP85 for each country you are talking about and not co-mingle foreign countries on one DPS85. You may end up with the DPS85 in Japan and you want to make another shipment to Korea. That means the license will have to be retransmitted to Korea before you can make your shipment. Finally, Mr. Fields said that a certain contractor on the West coast was involved in one detention. The contractor will go unnamed but it was three detentions. I recommend strongly to you that you check your people who are traveling overseas to make sure that they know what is in their possession and that they know what the authority is for carrying those items. By in their possession, I mean not only in their briefcases but also in their luggage. Both items are being checked and if they are taking technical data and you are claiming an authority under a certification that is one thing. If they are taking hardware, say at the last minute a PC board fails and somebody gives them a board to slip into their luggage to carry over to Germany, there is no exemption available. You will need a license and a shipper's export declaration. And be very, very careful that they follow that.

I list for your considerations which should be thought out each time you receive a foreign visitor. First, the sponsorship. (By sponsorship I am not using the word in the sense that the U.S. military services use it when they say sponsor the visit.) I am using it in the sense where the foreign government or the foreign activity says that this visitor officially represents an organization who is going to be coming to your facility and he does officially have a purpose. So that is what I mean by sponsorship.

The access eligibility you would probably know more commonly as a security clearance. Has a determination been made that that government is eligible for that information? Finally, does he have a need to know? The need to know principal is ignored too much today. For an industry standpoint it is the only way we have of protecting proprietary information.

We have broken down the types of visits, by the type of information that would be involved. We really have visits that are limited only to publically available information. The Department of Commerce regulations permit unclassified technical data to go to most countries except the Soviet Union and its aligned countries.

The third is something that causes us a deep concern each time our marketeers go out because we must have prior approval before our people make a proposal for the sale of products with a value over 7 million dollars, or for the assembly and production of significant combat equipment for which there is no dollar threshold. Does everyone know what significant combat equipment is? If you don't you should read the International Traffic in Arms Regulations (ITAR) and identify from the ITAR your products. Any item which is significant combat equipment is subject to the requirement of having prior approval before you make an offer to sell the equipment or an offer to enter into a production or assembly agreement. If you don't have that prior approval your license may be denied and you are in violation of the law and the possibility is the proposed arrangement will not be completed.

Finally, there is ITAR controlled technical data. We are not talking necessarily about technology, we are talking about technical data as defined in the ITAR, and for that you would need either a export license or an exemption. There is a misconception within the Department of Defense that

every foreigner visiting the contractor must be processed and be sponsored by the Department of Defense. I wish to dispel that, at least our facility has not been nationalized and we look upon visitors to our facility to include perhaps the Department of Defense. We control visitors coming in and we will determine what access they can have according to the U.S. laws. If we can have the visit in accordance with this then we do not need any further approvals.

Now lets go to the classified visits. This is where you get into some controversy. First of all consider the foreigner who owns classified information. What authority does he need to have access to his information at your facility? Secondly, consider classified information which was of U.S. origin but has been formally transmitted and given to the foreign government. He has placed it under his security procedures and according to the security agreement, he has executed, he is handling it according to his procedures. If he is handling it according to his procedures then who sponsors the visit? Who determines what access is going to be allowed and how do you know the proposed visitor is authorized to have access? With reference to classified NATO information, there is a procedure in paragraph 51c of the Industrial Security Manual that talks about how NATO visits are to be processed. Regardless of what the Department of Defense tells you, the ISM provides for how NATO visits are to be arranged. These do not require a visit authorization from the military service. I'm talking particulary in our case the foreign Air Force liasion. There is a procedure for the visit to be processed and it is not through U.S. military liasion offices.

Finally, how to handle U.S. classified information. The summary of all of this is if you were able to identify what information is going to be involved in the visit you can limit that visit to the prearranged levels. There is a strong probability that very few of the visits to your facility will ever have to be processed through the military service foreign liasion office. Only those which involve U.S. classified information and at least at our facility that amounts to less than 10% of all the visits to our facility. I think it is essential that you become involved in knowing what information is going to be involved to be disclosed and discussed. You should also inform those who are going to be the custodians of the information as to what the limits are and that you operate accordingly. If you can operate without going to the military service liasion offices, you can save yourself a lot of time on processing visit requests because most of the time you don't even need one. That is the way to cut the corner. Only ask for it when you absolutely need it.

**Richard Williams**
**Chief, Industrial Security Program**
**Defense Investigative Service**

Basically what you need to process a visitor is to is plan ahead. Work with DISCO. DISCO observes on a standard visit a 6 day to 7 day rule. We are going to make it 5 days as soon as we can and 3 and 2 and whatever we can get it down to. But basically, if you have an emergency call DISCO. DISCO has a procedure they will share with you. They will send it to you, they will let you look at it and you can keep it. And basically what it says is come to us and we will telex it. We will go out on an accelerated basis. We will try to get it out for you and we will have you get that visit there as quickly as we can. Now the couple of things Ed has just mentioned I want to add to and that is one of the problems — look in the mirror. And the problem is paragraph 37D. When you give us the information its partly inaccurate, its incomplete. Please read the new Industrial Security Letter (ISL). I've got three items in there on visits. It takes us a long time because the foreign country takes time to process it. So get it to us early. The second thing is observe the requirements of paragraph 37D. Get us the information. Get us complete information. The third thing is just because a military department won't sponsor an unclassified visit which would of course give you export authorization does it mean that you as a U.S. firm can accept that visit abiding by the U.S. laws. Now I put that in the ISL, laid that out clearly and distinctly so you can take a look at it and get an idea of exactly how it fits together. This is a very confusing area. It's an area that is a lot of concern. If you are in an overseas environment our office of Industrial Security can help you out.

Therefore, I am saying to you that the government and industry should treat each other with mutual respect, work together and move the visits. We can do it. Thank you very much.

# Expediting Transmission of International Classified Shipments

June 1983

**Junius C. Layson**
Chief, Security Administration
The Boeing Company
Seattle, Washington

# Lessons Learned

(With Tears)

## Classified Contracts With Foreign Involvement

- **Start Planning Before Contract Award**
- **Identify Program, Schedule, and Security Requirements Immediately**
  - **Disclosure Approval**
  - **Document/Equipment Release Procedures**
  - **Communication**
  - **Transmission Procedures**
  - **Visit Procedures**
  - **Resident Foreign Nationals**
  - **Foreign Country Facility Clearance**
- **Identify Problem Areas Requiring Resolution**
- **Identify Government/Departments/Agencies Having Jurisdiction**
- **Plan Extensive Time for Coordination and Resolution of Problem Areas with U.S. Government Agencies**
- **Coordination with Foreign Governments may be Required - Determine their Security Requirements & Procedures**
- **Document All Requirements Thoroughly**
- **Prepare Detailed Internal Procedures for Employees to Implement**

---

# International Classified Shipments

**Two Examples Illustrate the Complexity of Problems which May be Encountered and Solutions Reached.**

- **NATO E-3A Co-production Program**
- **French E-3A Demonstration**


# NATO E-3A Program

- Co-production Program Involving U.S. and Foreign Contractors in Europe Requiring Access to U.S./NATO Classified Information
- Contract Requires Large Volume of Classified Data and Hardware to be Exported from U.S. to Europe
- Expedited Movement Required to Meet Contract Schedules
- Compliance with U.S., NATO and FRG Security Regulations Required

# International Classified Shipments

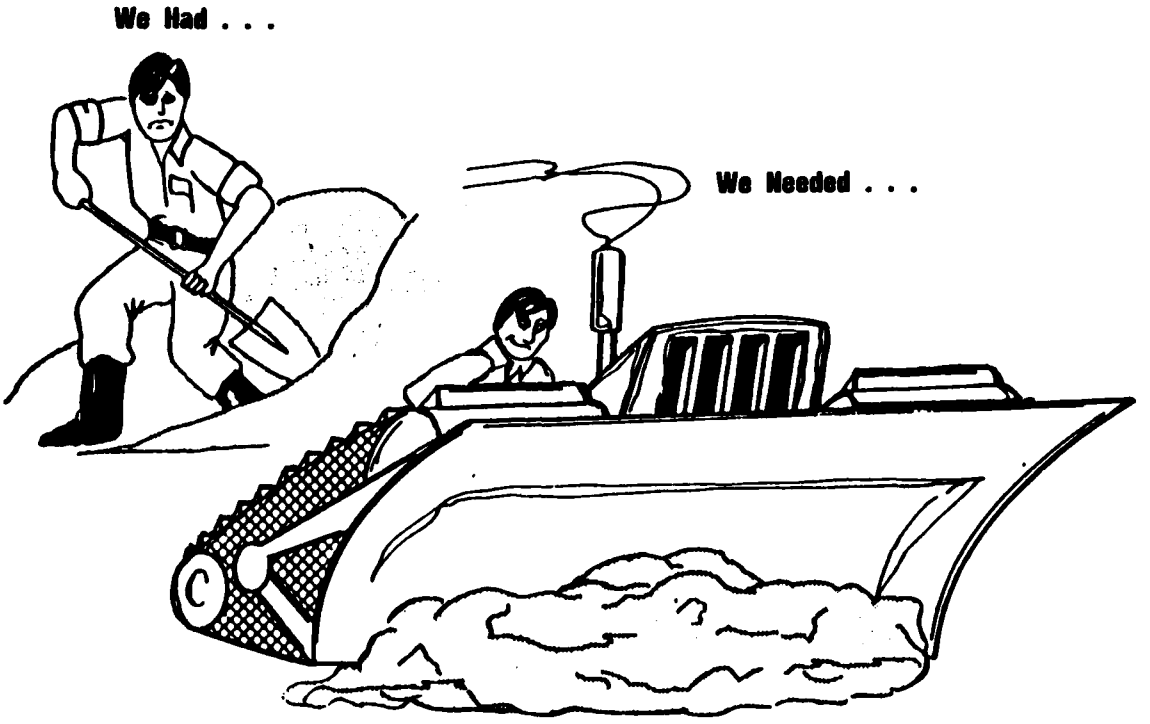
## NATO E-3A Co-production Program

**Major Problem Areas**

- Expeditious Export License Processing
- Expeditious Movement of Classified Material Across International Boundaries
  - Data
  - Hardware
    - Classified
    - COMSEC
- Airport Security and Customs Check of Couriers in U.S. and Europe
- Government-to-Government Transfer Point Locations

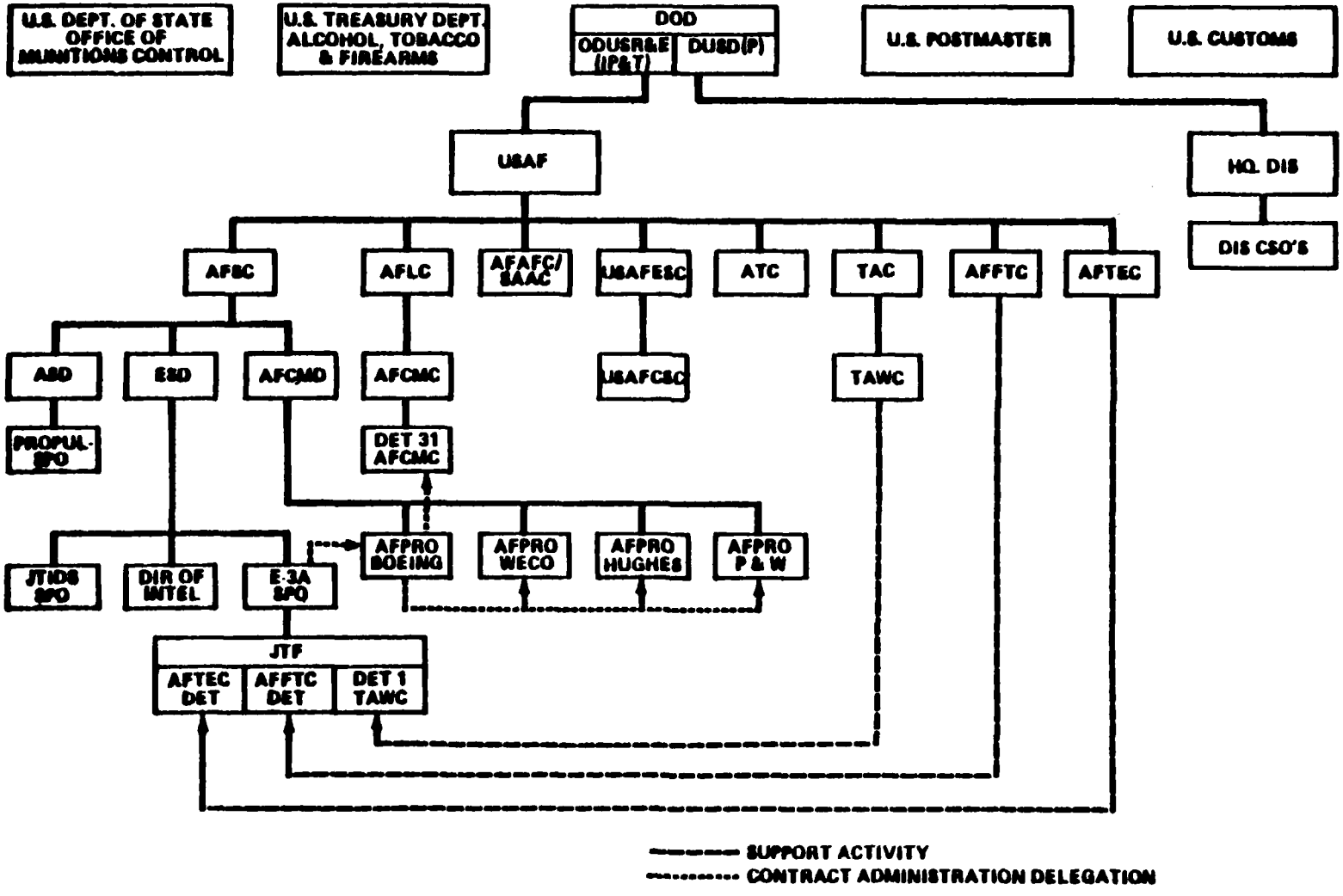
---

## We Learned



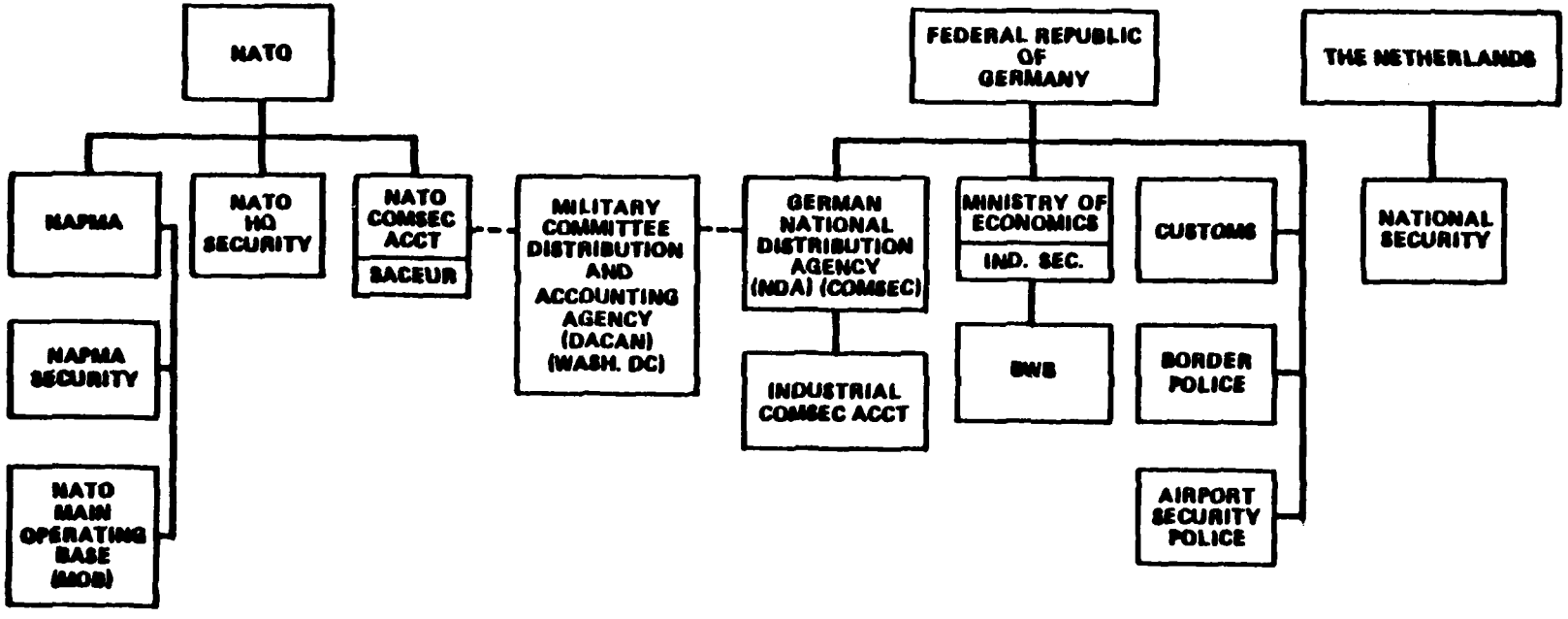
# NATO/E-3A Program

## Principle U.S. Government Agency Involvement



# NATO E-3A Program

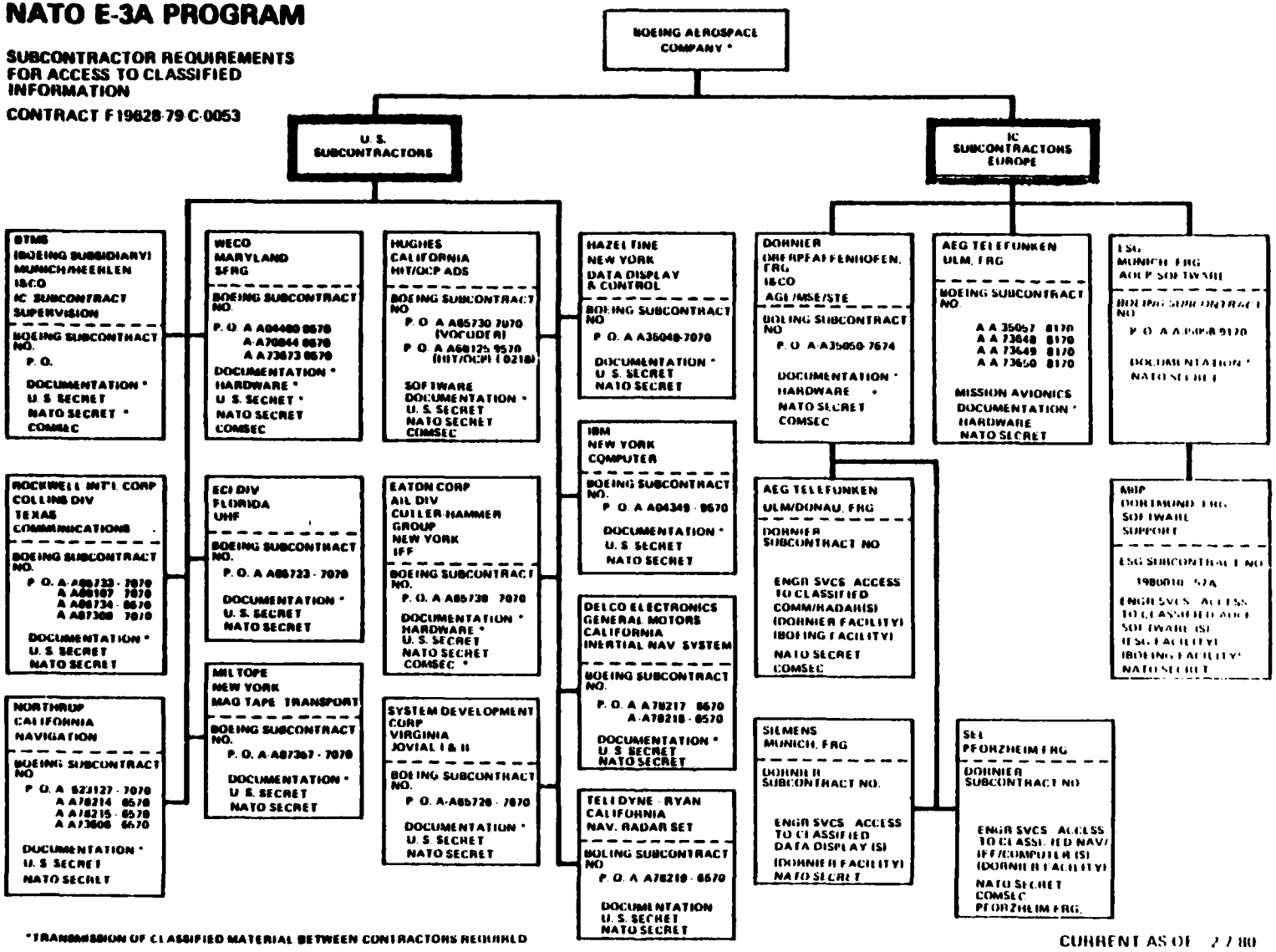
## Principle Foreign Government/International Pact Organization Involvement



# NATO E-3A PROGRAM

**SUBCONTRACTOR REQUIREMENTS FOR ACCESS TO CLASSIFIED INFORMATION**

**CONTRACT F19628-79-C-0053**

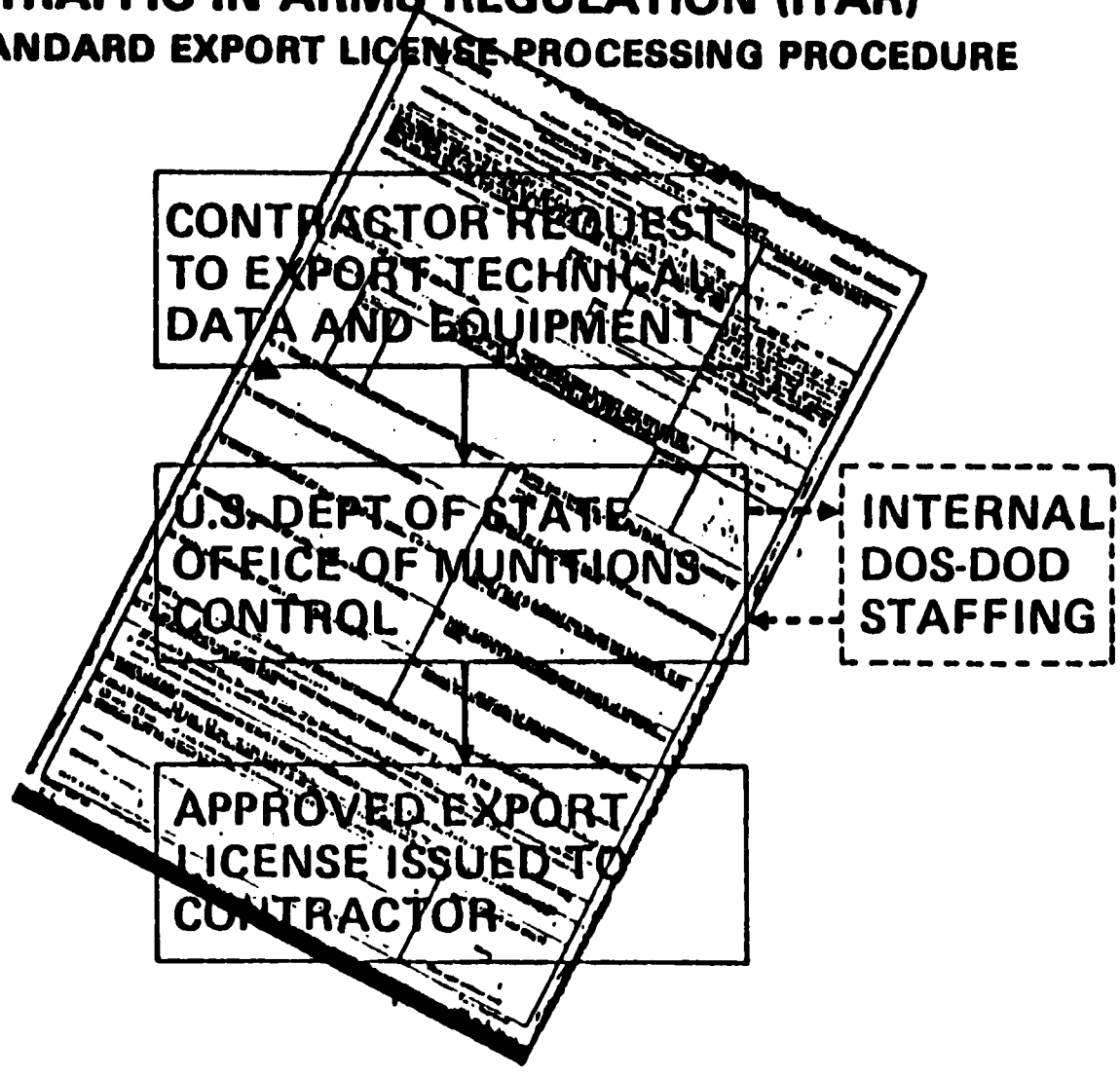



*TRANSMISSION OF CLASSIFIED MATERIAL BETWEEN CONTRACTORS REQUIRED

CURRENT AS OF 2/80

# INTERNATIONAL TRAFFIC IN ARMS REGULATION (ITAR)

## STANDARD EXPORT LICENSE PROCESSING PROCEDURE

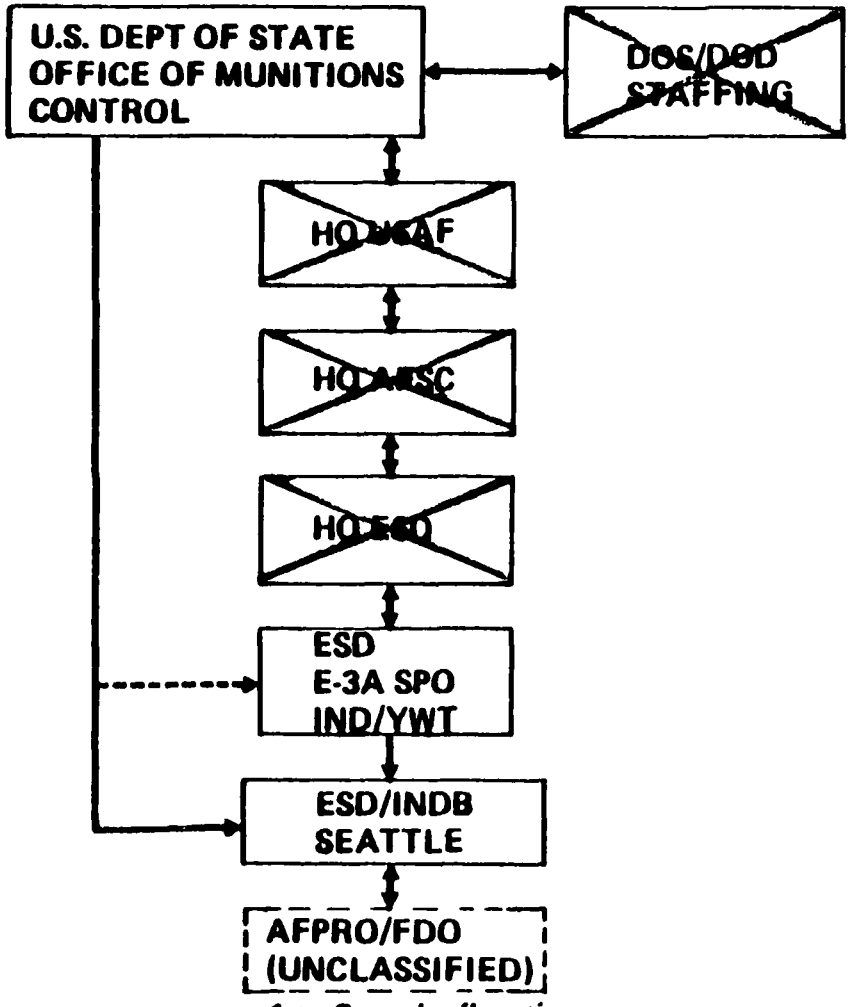



- Normal flow time—3 to 6 months

NATO E-3A

# NATO E-3A AGENCY AGREEMENT

## MANUFACTURING/TECHNICAL ASSISTANCE & EXPORT LICENSE FOREIGN DISCLOSURE re U.S. INFORMATION (EXPEDITED)



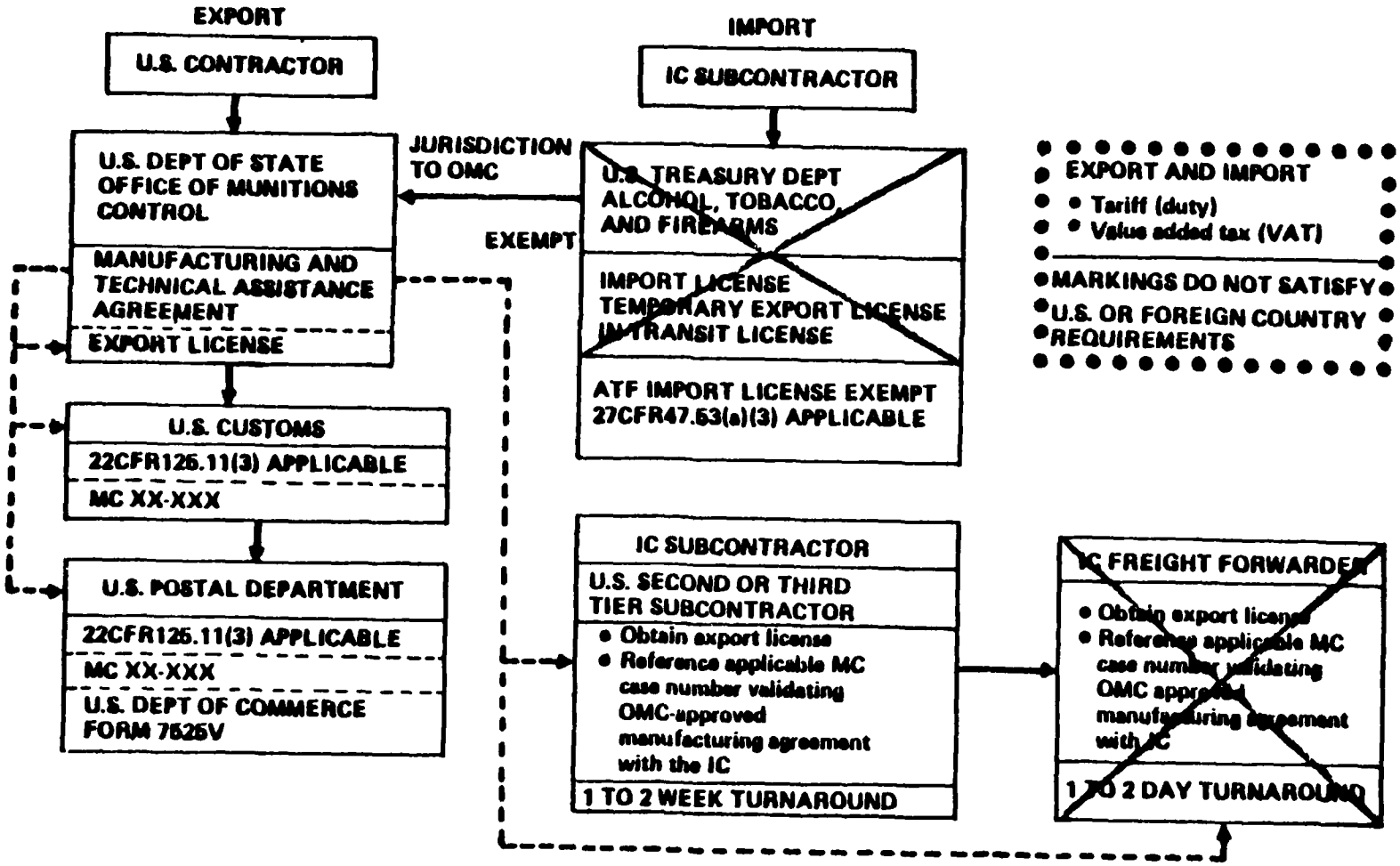

- 1 to 3 weeks flowtime

- Foreign disclosure policy established
- Contractor request for manufacturing and technical assistance or export license
- No OMC receipt or review of material concurrent with application
- In lieu of receipt or review, copy of NATO E-3A, DDT&E and production contracts and agency agreement to OMC
- Manufacturing and technical assistance or export license issued (conditionally):

  "The established control for review of both classified and unclassified data by AWACS (E-3A) SPO prior to release to foreign contractors is continued."
- ESD/INDB reviews and approves release; confirms approval to DS/OMC
- Process complete; export

NATO E-3A

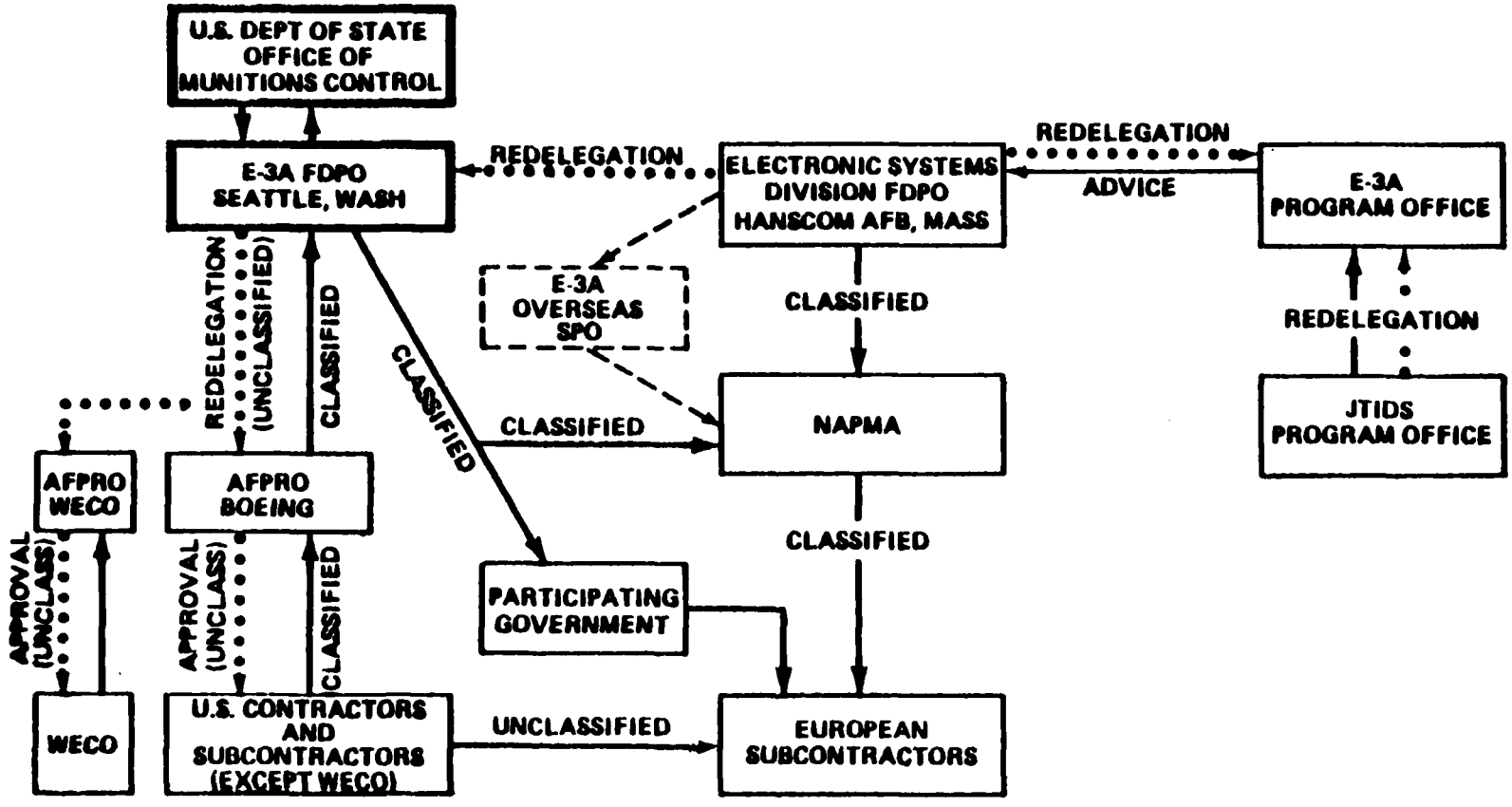
# NATO E-3A AGENCY AGREEMENT
## EXPORT/IMPORT CONTROL MECHANISMS (EXPEDITED)



NATO
E-3A

# NATO E-3A AGENCY AGREEMENT

## MANUFACTURING/TECHNICAL ASSISTANCE AGREEMENTS & EXPORT LICENSE FOREIGN DISCLOSURE APPROVAL (EXPEDITION




——— *Classified releases:* Government-to-government only

• • • • Unclassified releases: Directly from U.S. contractor to foreign subcontractor (with AFPRO - Boeing approval)

# International Classified Shipments

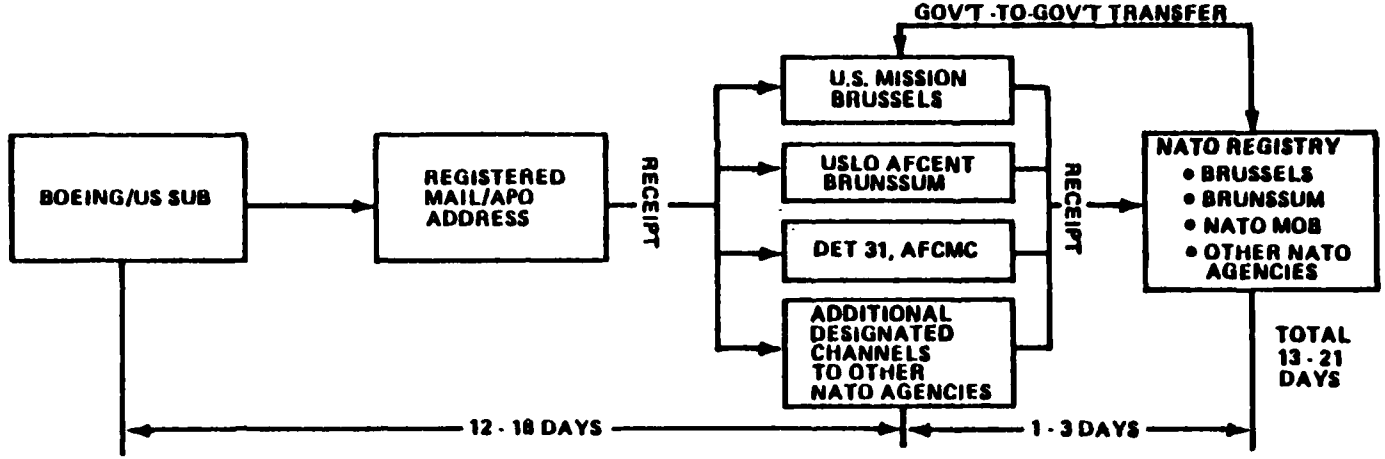
## Routine Methods of Transmission

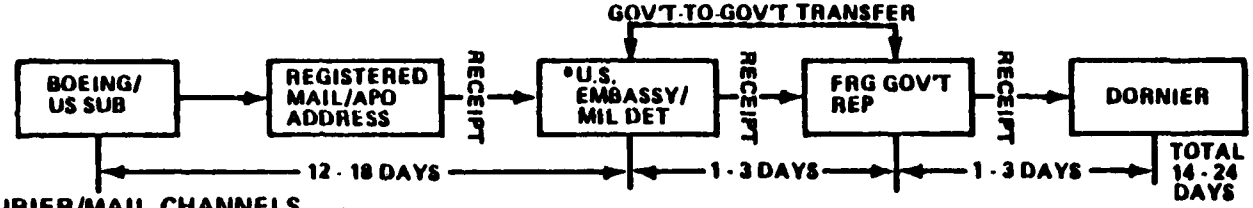
- U.S. Registered Mail
- U.S. Armed Forces Courier System (ARFCOS)
- U.S., NATO and/or Foreign Government Couriers
- U.S. Defense Transportation System (DTS)
- Foreign Embassy (Washington, D.C.)

# NATO E-3A Transportation Plan

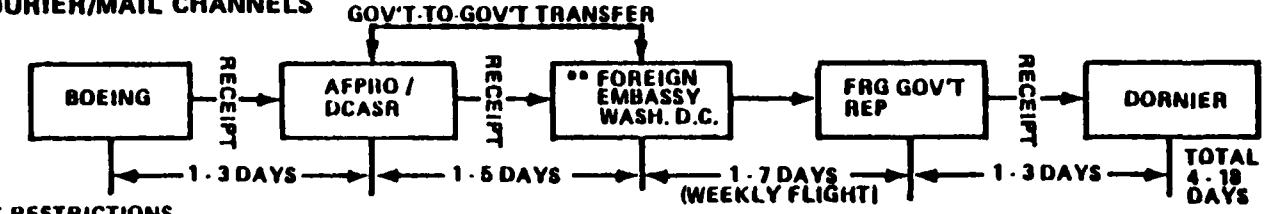
NATO E-3A

## REGISTERED MAIL CHANNEL




## COMBINATION U.S. COURIER/MAIL CHANNELS




- SIZE & WEIGHT RESTRICTIONS
  100" LENGTH & GIRTH
  MAXIMUM: 70 LB WEIGHT

* NEAREST U.S. AGENCY TO FOREIGN DESTINATION
** NOT CURRENTLY IN EFFECT - NATO/FRG AGREEMENT REQUIRED. MUST BE NEGOTIATED BETWEEN ESD/HQ USAF/NATO/FRG/ BOEING

# Expedited International Classified Transmissions Methods

- U.S. Contractor Personnel Authorized to be Appointed as U.S. Government or NATO Couriers to Transport Classified Material Across International Boundaries. Authorization Expanded to Authorize Use of U.S. Subcontractor Personnel in Addition to Prime Contractor
- Participating NATO Country Commercial Passenger Aircraft Authorized in Lieu of "U.S. Flag Air Carriers" Only
- Arrangements Made with U.S. and Foreign Commercial Airlines to Permit U.S. Courier Constant Surveillance of Classified Shipment During Airport Loading/Unloading Procedures
- Arrangements Made with Foreign Government for Exemption from Customs Inspection at Airport Entry Points
- Arrangements made with U.S. and Foreign Government for Central Government-to-Government Transfer of Classified Material (U.S. Courier, U.S. Government Representative, FRG Government Representative, FRG Subcontractor)
- Obtained Modified NATO/FRG COMSEC Transmission Channel and Accounting Procedures
- Expanded Use of DTS Insertion Points to Include Subcontractor Locations

USAREUR Regulation 55-355
CINCUSNAVEUR Inst. 4600.7C
USAFE Regulation 75-4

Part Five - Customs

Chapter 23 - Customs Procedures in Europe for U.S. Forces Official Consignments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
CAMERON STATION
ALEXANDRIA, VIRGINIA 22314

IN REPLY REFER TO DLA-MS

26 MAR 1980

SUBJECT: Request for Waiver, The Boeing Company, Seattle, WA

TO: Commander
DCASR, Los Angeles
ATTN: DCRL-1

1. The Boeing Company requested by letter of 9 August 1979, a copy of which has previously been furnished your Headquarters, expansion of the terms of the waiver granted them by our letter of 20 April 1979. In accordance with paragraph 1-114, Industrial Security Regulation, the Director, Security Plans and Programs, DUSD (Policy Review), has granted Boeing's request subject to the procedures identified in the enclosure.

2. The enclosed procedures, which have been coordinated with the Department of the Air Force, will permit the E-3A NATO Systems Program Director at HQ, Electronics Systems Division, AFSC, Hanscom Field, MA, to designate contractor employees to transport U.S. classified information or equipment across international boundaries. This authority will be granted only when an urgent situation exists in Europe, as determined by the U.S. Air Force.

3. It is requested that this determination and the enclosed procedures be provided to The Boeing Company and that adherence with the terms of same be made a matter of special attention during recurring industrial security inspections.

FOR THE DIRECTOR:

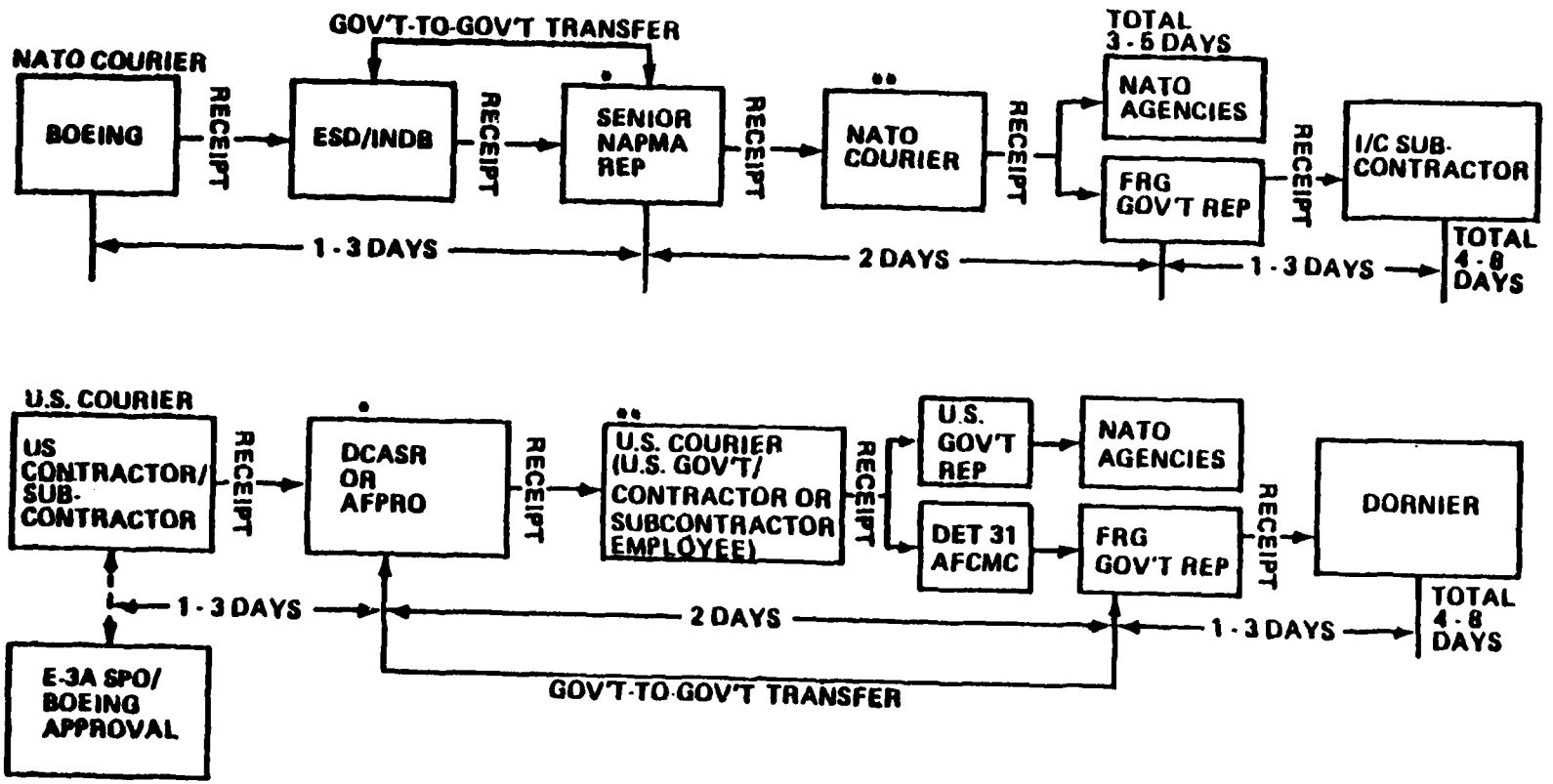
1 Encl

R. A. MAULDIN
Captain, USN
Executive Director,
Industrial Security

cc: AFOSP, Kirtland AFB NM
w/encl

# NATO E-3A Transportation Plan

URGENT SITUATIONS -- COURIER CHANNEL
(CLASSIFIED SHIPMENTS)




• ISSUES COURIER AUTHORIZATION TO CONTRACTOR EMPLOYEE

•• CONTRACTOR EMPLOYEE ACTING AS AN OFFICAL COURIER

# USAREUR Regulation 55-355
# CINCUSNAVEUR Inst. 4600.7C
# USAFE Regulation 75-4

## Part Five - Customs

## Chapter 23 - Customs Procedures in Europe for U.S. Forces Official Consignments

| REQUEST FOR EXPORT/IMPORT CUSTOMS DECLARATION AE FORM 302 | | DATE 16 NOV 80 |
|---|---|---|
| REQUESTING AGENCY: | DET 16, USAF CMC, MCGRAW KASERNE O/L MUNICH | |
| TRANSPORTER: | FLYING TIGER LINE | |
| MODE OF TRANSPORTATION: | COMMERCIAL AIR | |
| CONSIGNOR: | USAF AFPRO/FDO, SEATTLE, WASH., U.S.A. | |
| CONSIGNEE: | DET 16, USAF CMC, O/L OBERPFAFFENHOFEN (AT DORNIER) | |
| NUMBER AND DESCRIPTION OF PACKAGES | DESCRIPTION OF GOODS | WEIGHT |
| 1 | 2 EA. ELECTRONIC MODULES, PART NUMBER | 489 LBS |
| | 204-11828-1 | |
| | | |
| THIS CLASSIFIED SHIPMENT IS ACCOMPANIED BY | | |
| BOEING COURIER JOHN J. SMITH. | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

EXAMPLE ONLY

ABOVE LISTED GOODS ARE TO BE USED OR CONSUMED BY A MILITARY OR AUTHORIZED MILITARY SPONSORED AGENCY

A. STEINER
TYPED NAME

/S/ A. STEINER
SIGNATURE

MAJOR, USAF, OFFICER IN CHARGE, DET 16 USAF CMC O/L MUNICH
GRADE AND TITLE

Printed by Stamp and Stamper, in 1979

| EXEMPTION FROM GERMAN CUSTOMS INSPECTION | | DATE<br>18 NOV 80 |
|---|---|---|
| CONSIGNOR<br>USAF AFPRO/FDO<br>SEATTLE, WASH., USA | U.S. MILITARY AGENCY TO RECEIVE SHIPMENT<br>DET 16, USAF CMC<br>O/L OBERPFAFFENHOFEN | REFERENCE (AE FORM 302 NO.) |

THIS IS TO CERTIFY THAT THE CONSIGNMENT OF GOODS, CONSISTING OF ELECTRONIC MODULES (rail cars, vehicles, packages) MARKED AS FOLLOWS AIR WAYBILL 023-71285911, CONTAINS EXCLUSIVELY MILITARY EQUIPMENT SUBJECT TO SPECIAL PROTECTIVE PROVISIONS ON SECURITY GROUNDS AND THEREFORE SUBJECT TO SPECIAL CUSTOMS TREATMENT, PURSUANT TO SUBPARAGRAPH (C) OF PARAGRAPH 5 OF ARTICLE 45 OF THE SUPPLEMENTARY AGREEMENT TO THE NATO STATUS OF FORCES AGREEMENT.

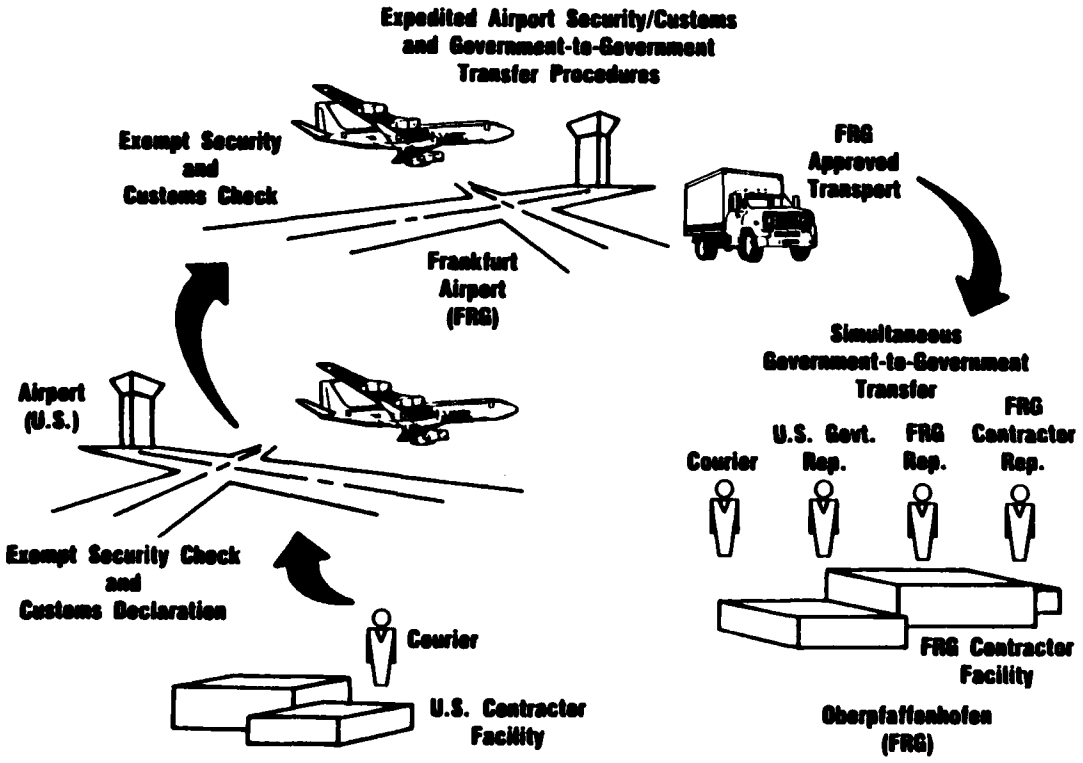
| OFFICIAL STAMP | TYPED NAME, GRADE, AND ORGANIZATION OF CERTIFYING OFFICER *(Field Grade Officer)* |
|---|---|
| EXAMPLE ONLY | A. STEINER, MAJ<br>DET 16, USAF CMC/OIC |
| THIS CERTIFICATE WILL BE VALID AFTER<br>*(Date to correspond with date of validity on U. Form 40.)*<br>18 November 1980 | SIGNATURE<br>/S/ A. STEINER |

THIS FORM WILL BE USED ONLY IN CONJUNCTION WITH AE FORM 302

AE FORM 3156
27 DEC 62

# International Classified Shipments

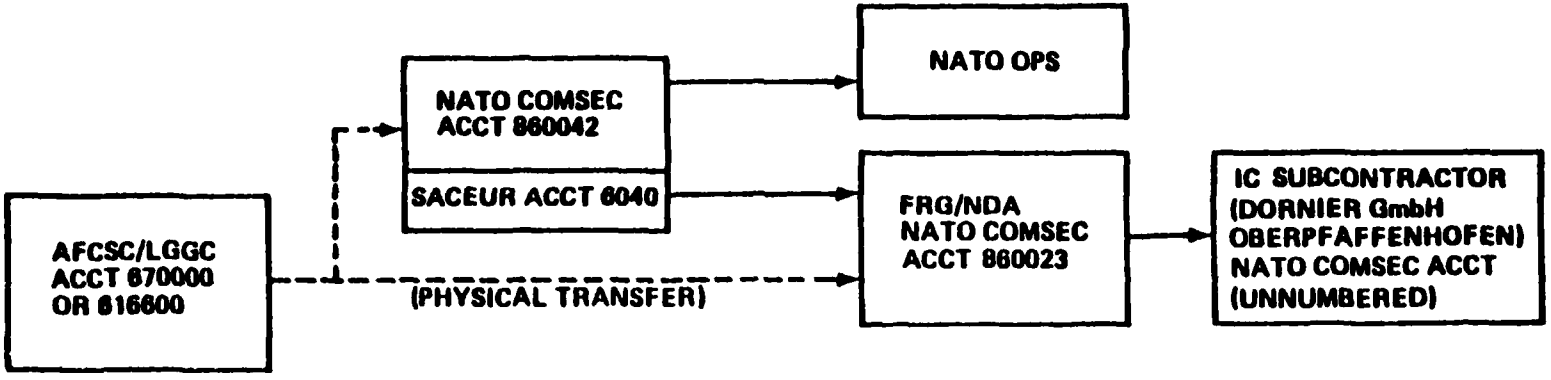
## NATO E-3A Co-production Program



NATO E-3A

# NATO E-3A TRANSPORTATION PLAN COMSEC MATERIAL FLOW

(CLASSIFIED OR UNCLASSIFIED)



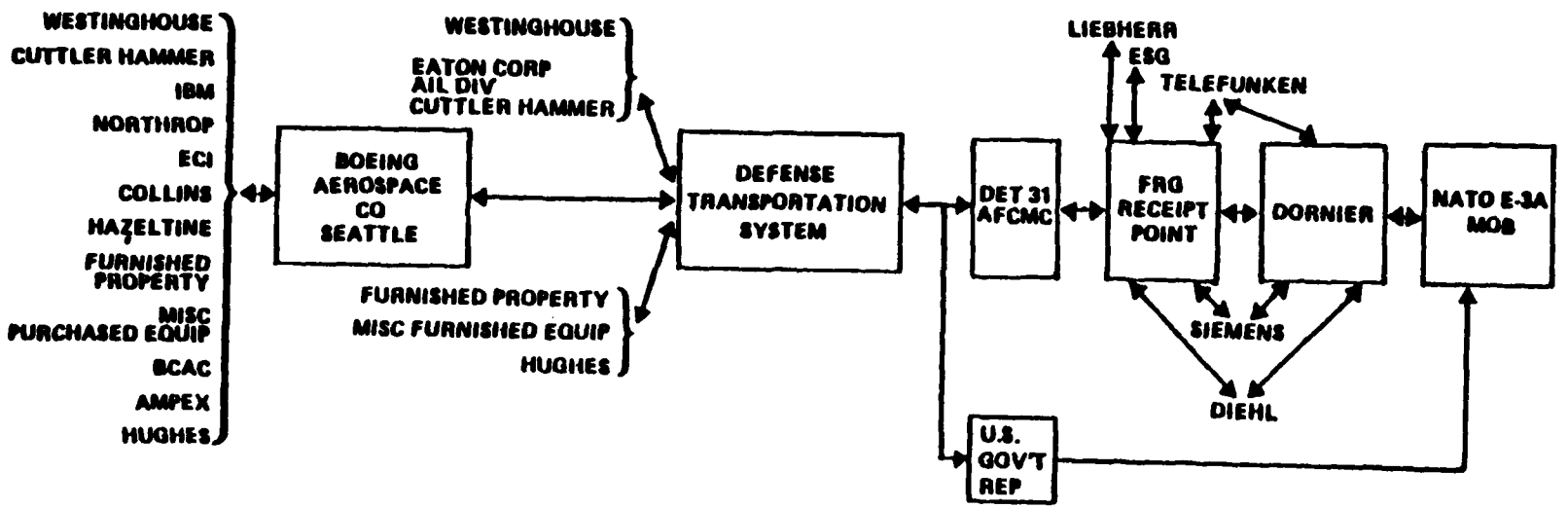
# NATO E-3A TRANSPORTATION PLAN

## CLASSIFIED HARDWARE SHIPPING FLOW (DTS)

**DTS INSERTION POINTS IN U.S.:**

| LOCATION | STATION CODE SYMBOL | LOCATION | STATION CODE SYMBOL |
|---|---|---|---|
| DOVER AIRFORCE BASE<br>DOVER, DELAWARE | DOV | KELLY AIRFORCE BASE<br>SAN ANTONIO, TEXAS | SKF |
| McGUIRE AIRFORCE BASE<br>WRIGHTSTOWN, NEW JERSEY | WRI | McCHORD AIRFORCE BASE<br>TACOMA, WASHINGTON | TCM |
| McDILL AIRFORCE BASE<br>TAMPA, FLORIDA | MCF | OFFUTT AIRFORCE BASE<br>OMAHA, NEBRASKA | OFF |
| NORTON AIRFORCE BASE<br>SAN BERNARDINO, CALIFORNIA | SBD | | |

**CONTACT: U.S.A.F. TRANSPORTATION OFFICE**



## French E-3A Demonstration


---

# International Classified Shipments

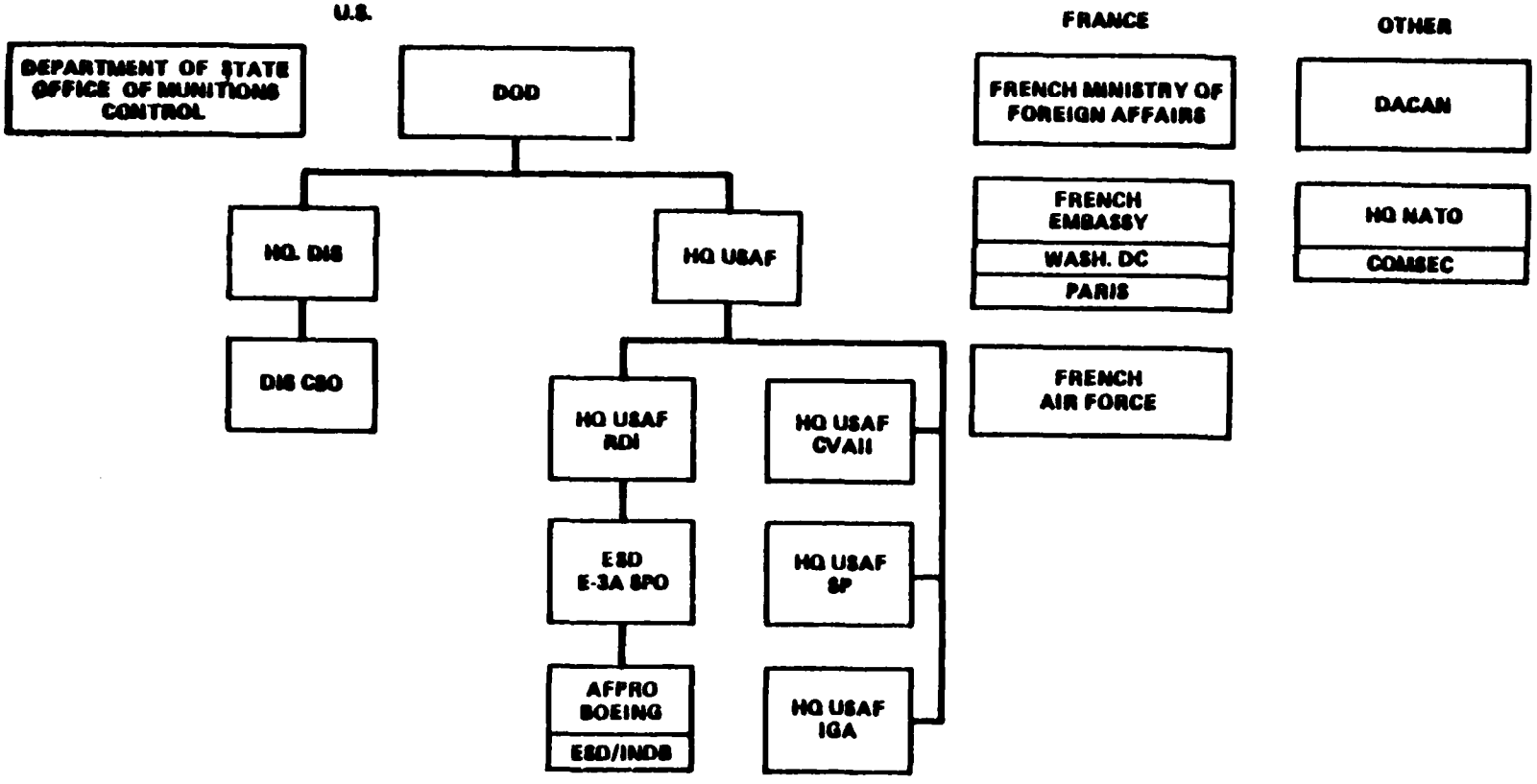
### French E-3A Demonstration
### (Temporary Export)

**Major Problem Areas**

- **E-3A Aircraft in Contractor Custody During Overseas Demonstration**
- **Storage of U.S. Classified Information in France**
  - **Test to be Conducted at French Air Force Installations**
  - **No U.S. Installation in Vicinity**
- **Government-to-Government Transfer of Classified Information**
  - **Encrypted Air-to-Ground Transmission**
  - **Temporary Exchange at Ground Test Site**
  - **Permanent Transfer**

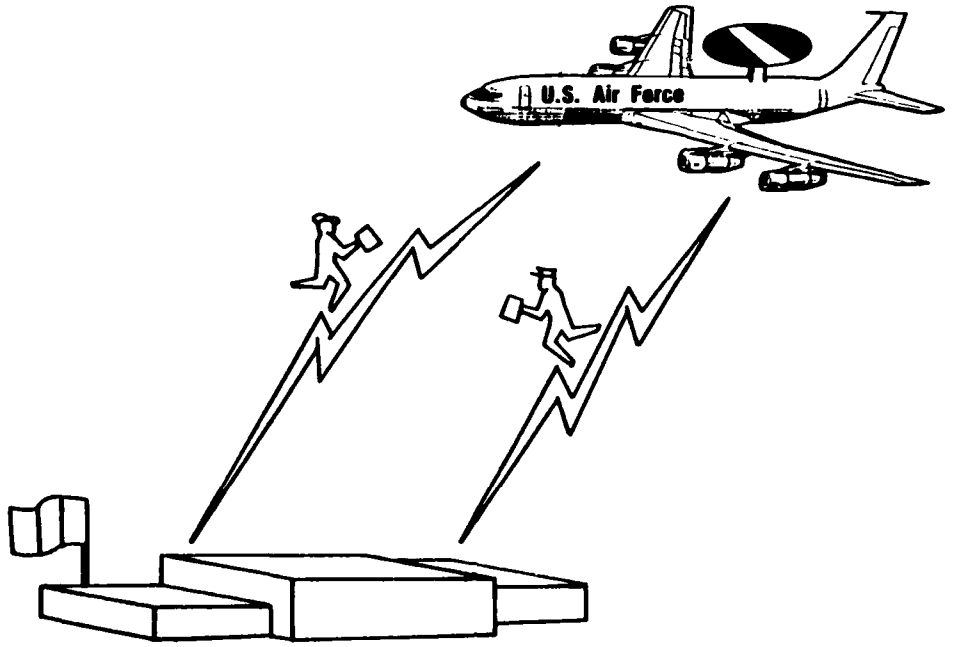
# French E-3A Demonstration

## Principle U.S./French Government Agency Involvement



# French E-3A Demonstration

**Classified Transmission (Encrypted)**




**French Ground Station**

DEFENSE INVESTIGATIVE SERVICE

April 23, 1982

S5210

Mr. John V. Clark
The Boeing Company
P.O. Box 3707
Seattle, WA 98124

Dear Mr. Clark:

Reference is made to your letter, March 30, 1982, subject: Request for Waiver/Approval of Security Procedures for Temporary Export of U.S. E-3A Aircraft to France for Test Demonstration Purposes.

In view of the unique conditions evident in your request, the Director, Defense Investigative Service has granted a waiver to paragraphs 94c(2) and 17e, Department of Defense Industrial Security Manual. The waiver was granted pursuant to the provisions of paragraph 1-114 Industrial Security Regulation. It is limited to this test/demonstration and contingent on:

a. The Air Force disclosure authorization to release the test data and related classified necessary for the demonstration.

b. Boeing providing cleared employees to ensure constant surveillance at the aircraft during non-duty hours, weekends and whenever the aircraft is not operating under the control and custody of cleared U.S. personnel. The aircraft must also be locked when it is not operating.

Sincerely,

James C. Titus

JAMES C. TITUS
Acting Director,
Industrial Security

---

# International Classified Shipments

## French E-3A Demonstration
## Solution Reached

- **DOD Waiver of Paragraph 17e and 94c(2), DOD Industrial Security Manual Obtained**

**Waiver Authorized:**

- **Storage of U.S. Classified Information on French Air Force Base**
- **Direct Transmission of Classified Information Between the Contractor and French Government Representatives**

**Waiver Based on:**

- **Executed U.S.-France General Security of Information Agreement (GSOIA)**
- **Air Force Disclosure Authorization Approving Release of E-3A Test and Classified Data**
- **HQ DIS/AF Approved Security Agreement Executed Between the Contractor and Government of France**

# International Classified Shipments

## French E-3A Demonstration
## Solution Reached

- Security Agreement Provided that:
- Government of France would:
  - Designate a Security Representative for All Security Matters
  - Identify French Personnel Requiring Access to E-3A Aircraft
  - Provide Secure Areas on French Air Base, Ground Stations and Other Locations
  - Provide Military Guards and Physical Security Measures for E-3A Aircraft
  - Protect U.S. Classified Information in Custody per GSOIA
  - Establish Accountability Record and Receipting System for U.S./French Classified Data Temporarily Exchanged, Permanently Transferred, and Encrypted Transmissions
  - Provide COMSEC Keying Material for Secure Transmissions Between Air and Ground
  - Report Loss or Compromise of U.S. Classified Information Immediately
  - Provide Additional Security Support as Necessary

# International Classified Shipments

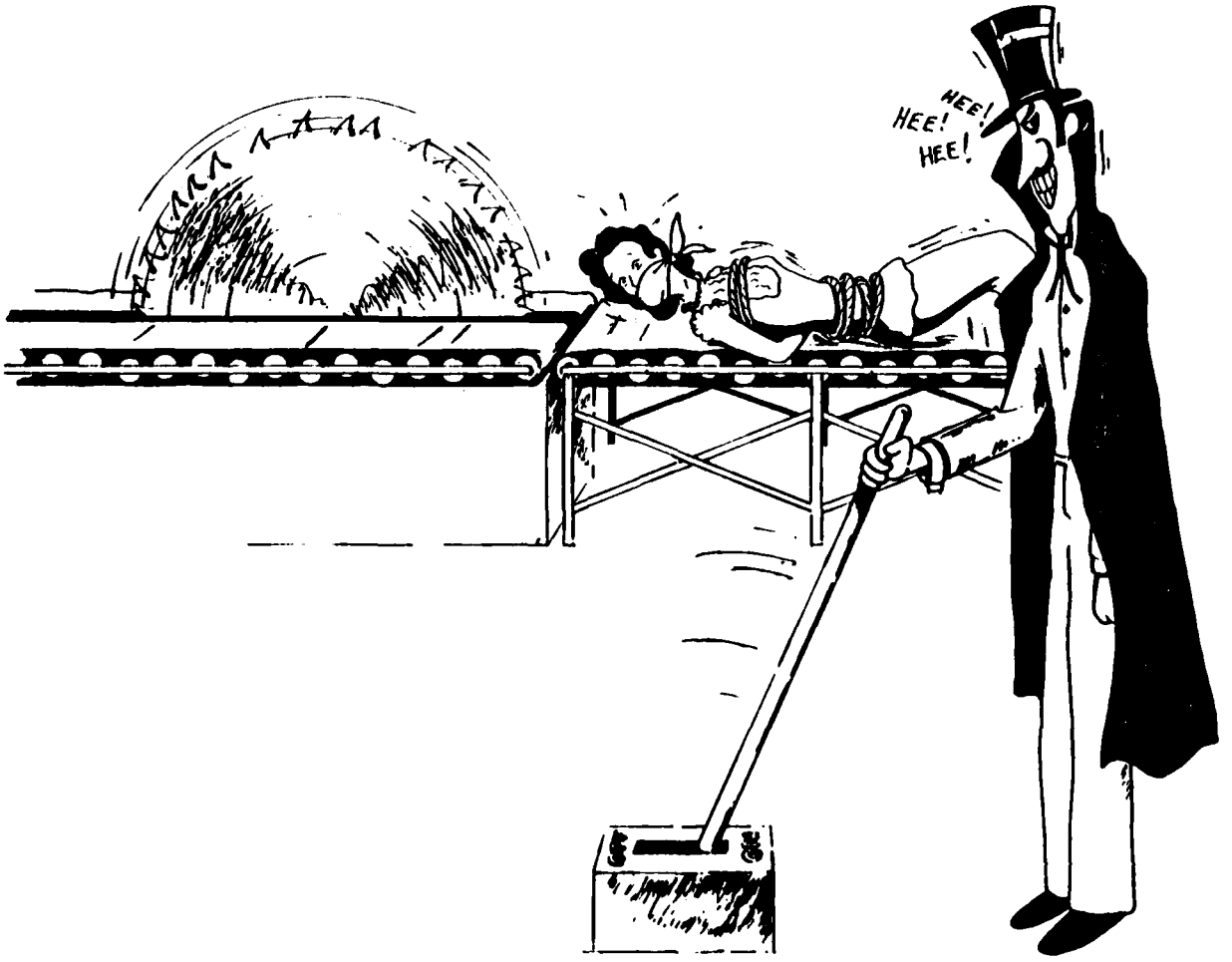
## French E-3A Demonstration
## Solution Reached

- U.S. Contractor would:
  - Designate a Security Representative for All Security Matters
  - Control Access to E-3A Aircraft During Work Periods - Lock Aircraft and Maintain Surveillance During Non-work Periods
  - Identify U.S. Personnel Requiring Access to French Air Force Base, Ground Station and Other Secure Areas
  - Protect French Classified Information in custody per GSOIA
  - Establish Accountability Record and Receipting System for U.S./French Classified Data Temporarily Exchanged, Permanently Transferred, and Encrypted Transmissions
  - Report Loss or Compromise of French Classified Information Immediately
  - Request Additional Security Support as Necessary

# International Classified Shipments

## Summary

- Identify Problem Areas Requiring Resolution as Soon as Possible
- Identify Problem in Detail to Government Agency Having Jurisdiction
- Provide Recommended Solution
    - Solution Must Provide Same or Better Security Measures as Currently Required
- Government Agencies will Assist in Finding Acceptable Solutions to Contractor Problems
- Plan on Long Lead Time to Resolve Complex Problems



# PART TWO

# Annual Report

# 1983

*19th Annual Meeting*

**Chris DeAngelis**
**President**
**National Classification Management Society**

Good morning and welcome to the 19th Annual Training Seminar. I should add one more thing- "Howdy!", because we are in the state of Texas. So at this time why don't we turn to the person next to you and give them a good 'ole Texas "Howdy!" It takes a lot do that, coming from the state of Connecticut. At this time I'd like to introduce to you our current Board of Directors: Our Vice President John Puckett with E-Systems; our Secretary Sandy Waller with DIS; our Treasurer Pam Hart with ALM Inc; Director and past President Jim Mathena with Martin Marietta, Cocoa Beach; Jerry Berkin with CNO; Irv Boker with GAO; Elaine Gruber, System Development Corp.; and Dick Fredlund, Dept. of Energy. We have two Directors absent: Jim Managee and Marilyn Griffin and also our Executive Secretary and Deputy Executive Secretary Gene and Barbara Suto, respectively. Gene could not be with us here at the seminar. He was just released from the hospital a few days ago and he is home recuperating.

I now call the 19th Annual Business Meeting to order. This brief meeting is held to share with you the status of Society Business. The first item of business is the membership report. I'll ask John Puckett to give that, please.

**John Puckett**
**Vice President NCMS**

"Howdy!" I'm a native son. I can say it good. Membership this year has been outstanding. We've got 697 regular members, eight life members, one honorary member, and five international members for a total of 711 members. That's outstanding, folks. We deserve a hand for each other. We've had a net increase, and we broke records in Florida last year, and since then we've added 144 members. That's just great. All areas and chapters have a gain. I hate to say this, but the guys in Florida came out ahead with total numbers and in gaining new members. We only had negatives in the New England region and the Hawaii Pacific Islands. New England dropped only 1 and they dropped 2 in the Hawaii area. We've just done great this year. We've had a total of 244 people join since last year. Once you drop the number of people that resign, retire or whatever, we come up with a net gain of 144. In the breakout for Industry, we have a plus of 109. We have a plus of 28 in Government. Other members and other categories-plus 7.

During 1975 to 1976, 37 people joined. From May 1982 to June 1983, 244 joined. The growth patterns from 1975 at 230 members goes to 711 this year. I can say without a doubt that this has been a fantastic year. I can't say that the membership growth has been steady and strong, it's been dynamic. It went straight up to the roof. It's great that the society is healthy. If you're not a member, we would strongly encourage you to consider membership. If you join at this seminar and you're a first time member when you join, we're going to waive the initiation fee. You can't beat that. Plus, the normal dues are only $40.00. However, we're going to give you a break. We're only going to charge you $20.00 because the year's half over. So for 20 bucks you can become a member.

**Madame President — Chris DeAngelis**

Thank you, John. Before you sit down I have a certificate of appreciation for you because you'll be ending your term of office on the board of directors. I'll read it to you. "John E. Puckett. For his expenditure of endless hours and abounding energies in the enhancement of his goals and the Society during the period 1980-1983. Mr. Puckett served the Society with distinction as National Vice President 1982-1983; National Secretary 1980-1982; Chairman Awards Committee, Chairman Membership Committee, Member Executive Committee, and Member of the Industrial Awareness Committee. Presented on the 21st day June 1983." Thank you very much.

The next item is the Treasurer's report and our Treasurer Pamela Hart will provide this.

**Pamela Hart**

Good morning. Your Board of Directors have budgeted for this year $58,050 for our operating account. To this date we have had expenditures

of $24,992.02. This leaves a balance of expenditures that I'll have to write checks for, or someone will, of $33,057.98. Leaving us with the net worth, based on those expenditures that we have not spent yet, of $22,849.77. Thank you very much.

**Madame President — Chris DeAngelis**

Thank you, Pam. Our by-laws require that we annually appoint a finance committee to review the financial records of the Society. This year Irv Boker was the Chairman of that committee and I'll ask him to give a report.

**Irving Boker**

The Finance Committee (Liz Heinbuch, Alan Thompson, and I) reviewed the Treasurer's records for calendar year 1982, and we found that the expenditures were properly vouched for and that the Society is in excellent financial condition, and has a bright future. We are earning all kinds of money on interest because our Treasurer has invested our excess funds very profitably in Virginia bank (Federally insured, I hope). That concludes the Finance Committee's report for this year.

**Madame President — Chris DeAngelis**

Thank you, Irv. Next is the announcement of the election results for the Board of Directors. Andrea Wraalstad, who chaired the committee is not here at the seminar, but I'll provide her report. A total of 691 ballots were mailed out and a total of 391 were returned, which meant that we had 57% of our members voting. I'll introduce to you now the newly-elected Directors: John Puckett, Irv Boker, Dick Fredlund, Bill Johnson who's with the Army Ballistic Missile Defense Command, and Robert Moore with Martin-Marietta in Denver. Congratulations to all of you and I thank Andrea for chairing the committee. Last week I received a letter from Marilyn Griffin resigning from the Board of Directors, as she'll be unable to attend board functions. According to our by-laws, when a board member resigns, the runner-up in the most recent election is asked to fill the unexpired term. This is done with the concurrence of the Board of Directors. So the one year term remaining, for Marilyn's term, will be filled by Liz Heinbuch who's with the Department of the Army. Would you please stand, Liz. The newly constituted 20th Board of Directors held a preliminary meeting yesterday for the purpose of electing officers for 1983-1984. And now I'll announce them to you: your new President for next year will be John Puckett; the Vice President, Pam Hart; Secretary, Elaine Gruber; and our Treasurer, Irv Boker.

I'd also like to recognize and give special thanks to our Executive Secretary, Gene Suto and Deputy Executive Secretary, Barbara Suto. They're both not here today. Our former Publications Director, Jack Robinson. Thank you, Jack. And our Bulletin Editor who also isn't here today, Kyle Norwood.

At this time I'd like to introduce Chapter Chairmen and Area Coordinators. I'm going to read all the names because I'm not really sure if they're all here. From the New England area Bob Roberto; Mid-Atlantic, Ray Herot; Washington, Andrea Wraalstad, but she's absent; Southeast area, Bill Johnson; East and West Northcentral areas Lyle Brakob; Dallas chapter Jerry Acuff; Rocky Mountain, Betty Boutwell; Southern California, Tony Correia; Northern California, Donna Harvey; San Diego, Rosemary Anderson; Florida Peninsula chapter, Everitt Harriss; and Hawaii and the Pacific islands, William Ledford.

There is one group that the board can always count on for help the President's Advisory Committee (PAC). We're not fortunate enough to have all of them here today but I'd like to recognize and introduce those who are: Jim Mathena, who was President in 1981; Fred Daigle, who had two terms in 1973 and 1979; Al Thompson, 1978; Dean Richardson, 1976; Jack Robinson, 1975; and Jim Bagley, 1972.

It's a custom with the Society that we present the outgoing Directors with an award. I've already done John's, but I have two more to do. A Certificate of Appreciation for Irving T. Boker for his outstanding contribution to the Society as a member of the National Board of Directors during 1982-1983. During this time Mr. Boker served the Society faithfully and efficiently as Chairman of the Finance Committee, member of the Government Awareness Committee, and member of the Publications Committee. Dick, could you come

up please? A Certificate of Appreciation for Robert R. Fredlund, Jr. for his outstanding contribution to the Society as a member of the National Board of Directors during the period 1980-1983. During this period, Mr. Fredlund served with distinction and as a member of the Government Awareness Committee. Thank you.

We're also pleased at this seminar to have 5 International members here and I'd like to introduce them and ask them to stand, please: Robert Grogan from Canada; Michael Holton from the United Kingdom; John McMichael from the United Kingdom; and Charles Fainsbert and Elaine Huber with Microwave Semiconductor. It's nice to have you all here with us.

The Donald B. Woodbridge Award for Excellence was established in 1980. This award was established in the honor of Donald Woodbridge, a charter member of the Society who served as President, Chairman of the Board, Counselor, and now Counselor Emeritus. This award is to recognize excellence in the field of Security Classification Management, according to the high standards of Mr. Woodbridge. In 1981 this award was presented to the late Frank Larsen, and if I may add here the Society was saddened on his passing last August. We lost a fine leader in the field of security and a wonderful person. This year at our April board meeting the board unanimously voted to ratify the selection of the Woodbridge Award Committee. It is now a very distinct pleasure that I call to the platform the 1983 Awardee of the Donald B. Woodbridge Award of Excellence, Mr. Jack A. Robinson. I'd like to read to you now the citation on which this award is based:

"Mr. Robinson has been a major contributor toward the development of the Classification Management Program, as it now exists, by active and forceful participation and Society contributions toward development of Executive Orders 11652, 12065; providing testimony and back-up information to House and Senate Committees on proposed legislation; providing pertinent information to staff personnel of the interested congressional committees; providing advice and criticism to the Interagency Classification Review Committee; furnishing advice to the General Accounting Office and its oversight of classification practices through our government; and in development programs for the training and education of classification management personnel. Jack has had a major impact on the Society, serving as President of the Society, Director, Seminar Program Chairman, 1975 & 1977; the Journal Editor, the Bulletin Editor from 1972-1977; and the Publications Editor from 1972-1983. His untiring efforts toward enhancing the background knowledge of government, classification authorities, and industry classification managers is reflected in the numerous NCMS National and many seminars and various service-sponsored symposia, during which he made presentations on pertinent subjects which have stood the test of time and change. Jack's accomplishments go well beyond his contribution to NCMS. Rather, they extend to the National Information Security Program as we know it as set forth in the current executive order. His primary contributions in this area are to personnel in the highest levels of all branches of government. Particularly, those who generate policy resulting in proposed legislation, consider national international requirements for a viable information security program and create the framework by which it will be accomplished; and scrutinize and critique the existing program. Jack, in a large measure, has been responsible for establishing NCMS as a critical resource for professional classification management; and an instrument by which policy is carried out, personnel are educated and procedures are examined and tested. As a result of his continuing liaison with policymakers, at the highest level of government, NCMS is involved in security classification policy development as well as the implementation of that policy. Jack A. Robinson has been, is, and hopefully will continue to be a vital force in the art and practice of classification management. He is a unique and well-respected force in shaping an existing program, and is an important advocate and voice throughout the government and industry, for the need and effectiveness of good classification management. On behalf of the Society, Jack, I have this plaque for you and I'll read the citation. National Classification Management Society presents to Jack Robinson the Donald B. Woodbridge Award of Excellence for his significant contributions to the Classification Management Program through active and dedicated service to the nation and to the Society from 1968 through 1982 and this is presented in 1983. Would you like to say a few words now, Jack?

**Jack B. Robinson**

Madame President, and my colleagues, I am very honored. I am also most humbled. Particularly so, when I think of and consider those with whom I have worked over these many years, and collaborated, and considered their contributions. In fact, I said to President DeAngelis when she advised me of my selection that, were I to have been a member of the Board, probably I would not have concurred. I was speechless. Unfortunately, perhaps for you, I have recovered.

My purpose is not, however, to dwell on the past, but to encourage for the future. There is a dynamic represented in this award. Dynamics, as I need not tell you, are interactive. They're an interactive process requiring all to participate. Success, it so often is clichéd, reads success. Much more remains and is necessary in this field than has been gained, no matter that we hope some has.

Credibility of classification determinations remains a goal yet to be achieved on a broadly based scale. NCMS, and all of us who are members, cannot rest on such laurels as we may have won. Much is yet to be done. As past President Richardson noted, we need to work smarter. I would add, perhaps, a bit harder as well. Opportunities to affect the program favorably are, in fact, widespread. Often, however, they pass unnoticed. It may be the case of only a youngster to whom one explains a point, or assists in achieving of proper guidance. The youngster, I might add in my terms, as one becomes older (everyone seems younger). But this society, and you particularly, can provide both the help and the guidance that is necessary. I am convinced that NCMS has been a positive influence on this continuously evolving program. It must so continue. There is little doubt for those willing to consider and to assess the program as it evolved post-Korea — to just give you an idea of how old I really am — that a great deal of favorable progress has in fact been made.

Each of us here, and members who are unable to be here today has either an initial or continuing further contribution to make to this program for it to continue to evolve properly and to improve. These contributions are rewarding in many ways. The problems to be solved are complex. They are multidimensional, interdisciplinary, resistant to comprehensive solution and by all odds could be characterized as intractable. None of these is an excuse for inaction.

Do not give up easily. Do not become unduly discouraged. And, by all means, do not abandon ship. I am told it is leaking only from the top. Again, thank you for this honor.

**Chris DeAngelis**

It has been a busy year for the Board of Directors and the Society, and at this time, I would just like to highlight a few points with you.

Last May in Orlando, I expressed a desire to see our membership exceed the mark of 700. We have reached this goal and now have 711 members. I thank all of you and our Executive Secretary and Deputy Executive Secretary for your recruiting efforts.

In September 1982, the Board supported a successful mini-seminar of the Northern California Chapter. Many Board Members also had the opportunity to attend a very successful 2 day seminar in Washington, under the direction of Andrea Wraalstad. In January the Board met in Washington and had the opportunity to attend a Chapter meeting there. And in March of this year the Board traveled to Fort Mommouth, New Jersey — the first time we traveled to that area. We attended and supported a mini-seminar of the Mid Atlantic Region. I must say at this time that Ray Herot and Tom Connor did a tremendous job in putting that on. I thank both of you.

The Board established an International Affairs Committee. Briefly, this committee will review foreign applications for membership and assist NCMS members who have international problems to the extent authorized by the aims, and the purposes of NCMS. Jim Bagley, who is the Chairman of this committee will give details of this during his presentation on Thursday.

The Member's Education Support Committee was also established and Jim Mathena is chairing this. It was established to support NCMS members in developing effective classification management, information security, education and training pro-

grams, and to provide or make available E&T materials to chapters and areas, or to the members at large. The committee will obtain existing and/or new material and determine if they should be disseminated or made available to the membership. They also plan to coordinate any special E&T activities at seminars by distributing or displaying materials. And we on the Board strongly urge the members, or any member, who has education and training material to contact either Jim Mathena, Rosemary Anderson, Tom Connor or Joe Grau while you are here at the seminar. I will say that this is one area that we can all benefit from.

I would also like to commend Rosemary Anderson for her efforts in conducting an ongoing series of workshops in the San Diego area. These have been very effective, and other chapters and areas may want to consider this type of approach.

The Board has also been looking into many ways to improve the timely issuance of its publications. I had hoped that we would be back on schedule at this time. We're not, but we've made progress. I am sure that during John's term of office you'll see this happen.

Serving you as President this year has been an extremely challenging and rewarding experience for me. The credit for the accomplishments this year belong with a dedicated group and I owe a special thanks to the Board of Directors, the Executive Committee, the Executive Secretary and his Deputy, the Bulletin Editor, and to Jack Robinson. I thank all of you for the opportunity of serving you. I truly value the close association with so many dedicated people. NCMS members are truly a unique group.

Is there any further business to come before this meeting? If not, I will declare this meeting adjourned and turn it back over to Jerry. Thank you very much.

END

FILMED

8

DTIC